CYBER POWER:
ATTACK & DEFENSE LESSONS FROM LAND, SEA, AND AIR POWER

BY

E. LINCOLN BONNER, III, MAJOR, USAF

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2011

APPROVAL

The undersigned certify that this thesis meets master’s-level standards of research, argumentation, and expression.

DR. JOHN B. SHELDON (Date)

JOHN H. DAVIS, PhD, Lieutenant Colonel, USAF (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Lincoln Bonner grew up in Northern California. He received his commission in 1997 through the Reserve Officer Training Corps at the Massachusetts Institute of Technology, where he earned a bachelor's degree in Aeronautics and Astronautics with a minor in Biomedical Engineering. A distinguished graduate from Undergraduate Space and Missile Training in 1998, he went on to perform space-based missile warning duties as a Defense Support Program satellite crew commander and instructor. Following an assignment at Arnold Engineering Development Center leading space and missile development testing, he was selected to attend the US Air Force Test Pilot School. After completing the school in 2004, he performed flight test engineer duties on several developmental flight test programs and served as an operations officer for a flight test squadron. Major Bonner is a senior space professional with over 300 flying hours in various aircraft, including the F-16, T-38, and HH-60. He holds a master's degrees in Aerospace Engineering from the University of Tennessee. and a master's degree in Military Operational Art and Science from the Air Command and Staff College. In July 2011, Major Bonner was assigned to the Air Force Chief of Staff's Strategic Studies Group.

ACKNOWLEDGMENTS

I would like to acknowledge those who helped me prepare this manuscript and without whom it would not have been a success. First, to the librarians and staff at the Muir S. Fairchild Research Information Center, thank you for making my research task as painless and streamlined as possible. I would also like to thank my classmates, particularly Lieutentant Colonel Paul Maykish who served as a sounding board throughout the year and helped me to refine my thinking on war and strategy through our discourse. I would also like to thank those at the National Security Agency (NSA) and US Cyber Command who provided assistance in aiding me in my search for a good interview candidate. This thought brings me to Mr. Trent Pitsenbarger, Technical Director for the NSA's System and Network Analysis Center, who I wholeheartedly appreciate for his time, trust, and insight as an interview subject. Trent, thank you for being so open and accessible, as well as for your patience and initiative in the interview coordination process.

I am also especially grateful to the faculty and staff of the School of Advanced Air and Space Studies. Their work throughout the year helped me become a better scholar, officer, and strategist. It was through their efforts that I was granted the opportunity to make the most of my ideas in this thesis. Most critical in that process were my thesis committee, Professor John Sheldon and Lieutenant Colonel John Davis. Thank you Lieutenant Colonel Davis for the diligence and thoroughness in your editorial advice, it has improved the manuscript's quality immeasurably. Professor Sheldon, I sincerely appreciate all of your guidance, support, and feedback throughout the year. Our many hours of debate and discussion helped me hone my hodgepodge of ideas into a coherent work that I am proud of.

Most importantly, I express my sincerest gratitude to my wife. She endured with a smile my real and virtual absence as I endeavored to complete this thesis. She readily accepted the added weight of the responsibilities that I shed to focus on this work. Without her to ensure that I ate, slept, exercised, relaxed, loved and laughed, I doubt that I would have survived this year, much less thrive as I did.

ABSTRACT

Cyberspace is the newest warfighting domain, but heretofore it has been the nearly exclusive purview of technical experts, not warfighters. Consequently, much of the work on cyber power theory has eschewed the traditional concepts and lexicon of war in favor of language more familiar to technical experts in information communications technology. This convention stunts strategic thinking on cyber power and creates a barrier to cyber power's integration into joint military operations. For these reasons, this study advances the beginnings of a cyber power theory rooted in the lessons of war experience in the traditional warfighting domains of land, sea, and air. By examining cyber power through the lens of fundamental concepts like initiative, terrain, speed, and mobility cyberspace's similarities to the other warfighting domains emerge.

Cyber power combines qualities inherent to land, sea, and air power – making cyber power simultaneously distinct from, and analogous to, all three. This unique synergy is what separates cyber power from these other forms of military power. At the same time, similarities between cyberspace and the physical domains lets cyber power theory take lessons from past war experiences, as well as from the military theories of those like Carl von Clausewitz, Sir Julian Corbett, Sir John Slessor, and John Boyd. By rigorously observing when the analogies between cyberspace and the other domains apply and collapse, this study gleans some lessons from traditional experience and theory on how to seize the advantage on attack or defense in cyber power.

CONTENTS

INTRODUCTION

War is a matter of vital importance to the state: the province of life or death, the road to survival or ruin. It must be thoroughly studied.

Sun Tzu
The Art of War

Theory exists so that one need not start afresh each time sorting out the material and plowing through it, but will find it ready to hand and in good order…it will light his way, ease his progress, train his judgment, and help him to avoid pitfalls.

Carl Von Clausewitz
On War

The medium we know today as cyberspace is truly new. The medium's beginnings can be traced back to World War II when the first analog computer, Colossus, was invented to aid the wildly effective Allied code-breaking effort against Germany, codenamed ULTRA.[1] The development of cyberspace was slow, but reached critical mass in the 1980s when the Internet (a network of networks) supplanted the ARPAnet (Advanced Research Projects Agency net).[2] Since that time, the spread of computer networking has become ubiquitous in the developed world, and continues to expand world wide at a breakneck pace with the proliferation of mobile computing smart phones.

Conflict has already started in cyberspace. One of the earliest examples is the American sabotage on a Soviet oil and gas pipeline in the early 1980s.[3] A more recent example is the cyber attack on the Iranian nuclear program using the Stuxnet computer virus. The Stuxnet virus corrupted the control system for the centrifuges Iran had been using to enrich uranium, destroying or disabling the centrifuges in the process.[4] Western

[1] R. A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra and the End of Secure Ciphers* (New York, NY: Cambridge University Press, 2006), 205-06.

[2] Adam Brate, *Technomanifestos: Visions From the Information Revolutionaries* (New York, NY: Texere, 2002), 107.

[3] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, Chatham House Report (London, United Kingdom: The Royal Institute of International Affairs, 2010), 6-7.

[4] William J. Broad, John Markoff, and David E. Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (accessed 17 January 2011).

analysts believe that this cyber attack, in conjunction with other measures, has delayed Iran's nuclear weapons program until 2015.[5] This delay, achieved non-kinetically, is the best most experts believed the United States or its allies could have attained with an air strike on those same centrifuge facilities.[6] Cyber power is the ability to exploit cyberspace to create advantages and influence events.[7] As Stuxnet demonstrates, cyber power can produce strategic, operational, and tactical effects on par with the traditional violent means of conflict – land, sea, and air power.

Yet, cyber power theory appears to be lagging the pace of conflict. This is not unique to the cyberspace domain. Air power was introduced into conflict in World War I (WWI), but air power theory did not develop significantly until after the war ended when those who participated in or observed the conflict had the opportunity to reflect on those experiences. Giuolio Douhet's *Command of the Air*, Brigadier General Billy Mitchell's *Winged Defense*, and Sir John Slessor's *Air Power and Armies* were all published prior to the start of World War II (WWII). The recent 2007 cyber conflict in Estonia and the 2008 cyber conflict between Georgia and Russia, while significantly smaller in scope than WWI, offer an opportunity similar to that laid before air power thinkers in the Interwar Years – to develop cyber power theory through close examination of and reflection on real conflict.

Martin Libicki provides one of the best early works on the application of cyber power written before the cyber warfare experiences of Estonia and Georgia. His *Conquest in Cyberspace* is an excellent work, drawing on real examples of cyber attack, though these examples largely lie in the realm of criminal activity rather than war or coercive state-versus-state conflict. Additionally, he avoids drawing explicit lessons from traditional theory on military strategy, though these lessons are readily apparent throughout his work. For example, although Libicki does not credit Alfred Thayer Mahan or Billy Mitchell for inspiration, his discussion of hostile and friendly conquest in cyberspace shares striking similarities to Mahan's description of how to gain command of

[5] Broad, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay."
[6] Broad, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay."
[7] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press: Potomac Books, 2009), 38.

the sea, in war through combat, and in peace by creating and controlling critical infrastructure and terrain.[8]

Libicki's work suffers from a critique that can be levied against many of the authors writing about cyberspace today – they take the claim that cyberspace is different from the other warfighting domains of land, sea, air, and space too far. For example, in one of Libicki's newer works, *Cyberdeterrence and Cyberwar*, he states:

> The establishment of the 24th Air Force and U.S. Cyber Command marks the ascent of cyberspace as a military domain. As such, it joins the historic domains of land, sea, air, and space. All this might lead to a belief that the historic constructs of war – force, offense, defense, deterrence – can be applied to cyberspace with little modification. Not so. Instead, cyberspace must be understood on its own terms, and policy decisions being made for these and other new commands must reflect such understanding. Attempts to transfer policy constructs from other forms of warfare will not only fail but also hinder policy and planning.[9]

Libicki's basic premise, that cyberspace must be understood on its own terms, is as true for cyberspace as it is for every warfighting domain. However, while cyberspace has unique characteristics, warfare constructs from the other domains can be applied to cyber warfare. There is much transfer value from lessons learned about military operations in the physical domains, if one is disciplined about applying analogies based on universal concepts, such as speed and mobility, and if one appreciates the boundary conditions that validate those analogies.

Claims similar to those being made about cyberspace regarding the non-utility of historical warfare constructs were also made about the inapplicability of land warfare lessons to air warfare at the dawn of the aviation age during the 1920s and 1930s. The air power prophets Mitchell and Douhet made such claims. Unlike these earlier prophets, Slessor, in applying to air warfare the fundamentals of sea warfare, themselves based on

[8] A. T. Mahan and John B. Hattendorf, *Mahan on Naval Strategy : Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, Classics of Sea Power (Annapolis, MD: Naval Institute Press, 1991), 23. Naval strategy differs from military strategy because it is needed in peace and war, as in peace a state may be able to gain overseas positions by purchase or treaty that cannot be had through war.

[9] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Project Air Force (Santa Monica, CA: RAND, 2009), xiii.

the land warfare lessons as described in the works of Sir Julian Corbett and Mahan, explained the transfer value of land and sea strategic principles to the air domain.[10]

While there is some movement in the cyber literature towards looking to past conflict experiences in the physical domains for transferrable lessons, these comparisons are typically ad hoc and lack rigor. For example, contradicting his later assertion in *Cyberdeterrence and Cyberwar* about the transfer value of constructs from other domains, Libicki uses a land warfare analogy in *Conquest in Cyberspace* to describe and analyze defense in cyberspace. He employs castles as a metaphor for the defensive strategy of using firewalls to defend data in cyberspace.[11] Throughout his discussion, there is no mention of why this analogy is valid based on fundamental concepts and no attempt to examine historical uses of fortifications for defense. Libicki also does not analyze whether or not the use of firewalls conforms to generally accepted concepts, based on experience, surrounding the effective use of fortifications in land warfare. Future analysts need to avoid this type of omission when using analogies as cyber power develops. As the United States formalizes its approach to cyber power in strategy, doctrine, and organization, it is imperative the basis for this formalization be sound, founded on rigorous thinking, grounded in experience.

Another shortcoming in the cyber power literature is its focus on the use of cyber power as an independent entity instead of one element of power in a joint military campaign. These analyses have focused on attacking cyberspace vulnerabilities to compel a nation-state to do the attacker's will through total war executed via cyber means, in what David Lonsdale refers to as strategic information war in *The Nature of*

[10] John C. Slessor, *Air Power and Armies* (Tuscaloosa, AL: University of Alabama Press, 2009), 39, 44, 61-85. For example, Slessor uses naval terms (i.e. fleet-in-being and close blockade) to describe how to gain air superiority. Additionally, Slessor centers his discussion of strategic concentration in Chapter V around land power theorist Antoine Jomini's concept of the decisive point. Julian S. Corbett, *Some Principles of Maritime Strategy*, Classics of Sea Power (Annapolis, MD: Naval Institute Press, 1988), 15-87. Corbett's basis for his theory rests on Clausewitz's theory of war on land as he described in "Part I: Theory of War" of his book. Mahan and Hattendorf, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, 97-170. Mahan's discussion of principles, strategic points, lines of communication, and interior lines reflects Antoine Jomini's theory of land warfare.

[11] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 62-63.

War in the Information Age, but others more commonly call cyber war.[12] Cyber war treats the enemy state as a system and attacks all of a state's instruments of power (political, economic, and military) simultaneously, to include the civilian power grid, financial system, and transportation system.[13] With cyber war, one could theoretically achieve victory with dramatically reduced expenditures of blood and treasure. In this way, cyber war as a strategy appears strikingly similar to the strategic bombing, air power theories of victory that history has largely proven inapplicable in most contexts. Libicki debunks cyber war as a viable strategy in *Cyberdeterrence and Cyberwar*, concluding that cyber war is unlikely to be decisive (a conclusion shared by Lonsdale) while cyber power may facilitate or amplify physical operations in a joint military campaign.[14]

Cyber power has value in two ways for a joint campaign. First, it enhances, or in some instances is even the source of, cohesion.[15] In the lexicon of John Boyd, cyberspace itself is a harmonizing agent permitting a dispersed, heterogeneous force to act as a coordinated whole, and to do so rapidly.[16] Secondly, cyber power significantly aids in orientation, or estimates as Sun Tzu refers to them.[17] Orientation is the process of analysis (destruction), breaking down the situation, followed by synthesis (creation), developing a picture of what the situation is, how it is unfolding, and how one can take

---

[12] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York, NY: Frank Cass, 2004), 135. Strategic information war (cyber war) is the use of cyber power to attack and enemy's National Information Infrastructure. Like strategic bombing, cyber war seeks to bypass enemy surface forces to strike directly at the perceived center of gravity.

[13] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, 1st ed. (New York, NY: Ecco, 2010), 257-61.

[14] Libicki, *Cyberdeterrence and Cyberwar*, xiv-xv. Lonsdale, *The Nature of War in the Information Age*, 206-07. Although cyber war is a new form of warfare, in most circumstances it will merely act as a supporting element to traditional forces.

[15] William E. Young, Jr. quoted in John B. Sheldon (Professor, School of Advanced Air and Space Studies, Air University), interview by author, 17 November 2010.

[16] John R. Boyd, "Patterns of Conflict," in *A Discourse on Winning and Losing*, 27 February 2005 ed. Chet Richards and Chuck Spinney (Atlanta, GA: Defense and the National Interest, 1987), 78. A harmonizing agent is a "unifying concept that provides a way to rapidly shape focus and direction of effort as well as harmonize support activities with combat operations, thereby permit[ting] a true decentralization of tactical command within centralized strategic guidance – without losing cohesion of overall effort." Put another way, a harmonizing agent is a "unifying medium that provides a directed way to tie initiative of many subordinate actions with superior intent as a basis to diminish friction and compress time in order generate a favorable mismatch in time/ability to shape and adapt to unfolding circumstances."

[17] Sun Tzu and Samuel B. Griffith, *The Illustrated Art of War* (New York, NY: Oxford University Press, 2005), 103. Estimates are the calculations of the balance of forces that are the strategist's keys to victory.

the initiative to act upon the situation to one's advantage.[18] Lastly cyber power allows military forces to sort, correlate, and assimilate vast amounts of information. The computational capacity of cyber power allows one to consider more, and more complex, potential courses of action during the decision process at greater speeds. John Boyd, in *A Discourse on Winning and Losing*, explains that an organism's fitness stems from the entity's variety, rapidity, harmony, and initiative allowing the organism to readily adapt.[19] Cyber power enhances all of the qualities that contribute to a military's fitness. A joint military force capable of employing cyber power effectively raises its ability to better adapt to the complex, interactive environment of war. A joint military force, effective in its use of cyber power, increases its ability to win.

Cyber power as one component of a joint air, land, sea, space, and cyberspace force fighting towards winning a single campaign – cyber power in war – is the context for the following analysis. In that context, the objective of this work is to illuminate some lessons of cyber attack and cyber defense to support the more informed use of cyber power in military operations. These lessons are informed by comparisons of cyber attack and cyber defense as they were performed in the 2007 cyber power supported clash in Estonia and the 2008 cyber power facilitated joint military campaign in Georgia, against land, sea, and air warfare exemplars from the twentieth century from WWII to Operation Desert Storm. This discussion omits the space domain, because fortunately conflict has not yet followed into this arena, so no truly valuable exemplars of space combat exist to draw upon. The following analysis is grounded in the concepts of strategy described by Clausewitz, Corbett, and Slessor. As the discussion gleans lessons from other domains, the focus will be on the effect of a few universal contextual factors – terrain, persistence, speed, mobility, and intelligence. These factors affect warfare in all domains, but the relative importance of each factor in a given domain differs. As cyberspace is unique, it is analogous to no single physical domain across all of these

[18] John R. Boyd, "Organic Design for Command and Control," in *A Discourse on Winning and Losing*, February 2005 ed. Chet Richards and Chuck Spinney (Atlanta, GA: Defense and the National Interest, 1987), Boyd, "Patterns," 14-15. Orientation is an interactive, implicit process that shapes the character of the present, and thus the way we act. John R. Boyd, "Conceptual Spiral" (1992), in *A Discourse on Winning and Losing* (Atlanta, GA: Defense and the National Interest, 1987), 22-40. Analysis and synthesis is the feedback process through which orientation mismatches with observation are resolved to produce better orientation.

[19] Boyd, "Patterns," 11-12.

fundamental factors. Regarding the use of terrain and fortifications, cyber power shares similarities to land power. Regarding persistence, cyber power shares similarities to sea power. Regarding speed and mobility, cyber power shares similarities to air power. Lastly, regarding intelligence cyber power shares similarities to both sea and air power.

The discussion begins with a description of fundamental attack and defense concepts, particularly the initiative, terrain, and concentric attack. This is followed by a detailed description of the cyber battlespace and its similarities to the land, sea, and air domains relative to the universal factors of terrain, persistence, speed, mobility, and intelligence. The specific uses of cyber power underpinning this work, the 2007 and 2008 conflicts in Estonia and Georgia respectively are then described. For comparison, elements of these cases are then related to lessons drawn from the land, sea, and air domains using battles from WWII, the Korean War, and the 1991 Persian Gulf War.

CHAPTER 1

CLAUSEWITZ'S FUNDAMENTALS OF ATTACK AND DEFENSE

The concept of defense is parrying a blow.[1] The object of defense is simple, preservation.[2] The objective of any defense is to preserve that which the defender values. The reason one assumes the defense in the first place is the value of waiting.[3] Thus the characteristic of defense is awaiting a blow.[4] If a defense deters an aggressor from attacking, waiting has served its purpose and the object of defense, preservation, is achieved.[5] Should an adversary be undeterred and attack, the defender should only remain on the defense so long as waiting for the situation to become more favorable is more valuable than an immediate counterstrike.[6] While on the defense, one may lose things of value, but the defense may scrap everything of value if it mounts a counterattack prematurely.

Clausewitz identifies six determinants of advantage in strategy, whether on attack or defense: surprise and initiative, terrain, whether one has the ability to apply concentric fires on the enemy, whether the theater of operations has been strengthened with fortresses, popular support, and exploitation of moral factors.[7] Strategy is the use of military engagements for the purpose of war, to compel the enemy to do one's will.[8] Of these determinants, surprise and initiative are of critical importance. Artfully used, initiative can bring a conflict to an end in a single stroke.[9] Initiative is the key to successful attack or defense. Initiative is the ability to surprise an opponent, which often reflects the ability to choose the conditions of battle, or stated another way, initiative

---

[1] Carl von Clausewitz, *On War*, ed. and trans. Michael Eliot Howard and Peter Paret (New York: Oxford University Press, 2006), 357.
[2] Clausewitz, *On War*, 357.
[3] Clausewitz, *On War*, 357. Because any omission of the attack accrues to the defenders' benefit, time accumulates to the defender's credit.
[4] Clausewitz, *On War*, 357.
[5] Clausewitz, *On War*, 357.
[6] Clausewitz, *On War*, 358. Defense "should be used only so long as weakness compels, and be abandoned as soon as we are strong enough to pursue a positive object."
[7] Clausewitz, *On War*, 363.
[8] Clausewitz, *On War*, 75,128.
[9] Clausewitz, *On War*, 363.

often reflects the ability to offer or refuse combat according to one's desire.[10] All successful military operations are in some way rooted in the advantage of surprise – rooted in which side has the initiative.[11]

Initiative is the key to success. Terrain, concentric fires, fortresses, popular support, moral factors, these all affect which force has the initiative in a conflict. Clausewitz exalts that above all else, the defense must seek to keep the enemy under observation, and the defense must be ready and able to fling himself upon the enemy.[12] When the defense can do this, it accrues an advantage with respect to initiative, or at least minimizes the attack's initiative advantage. The side with the initiative acts with greater certainty, while the side without the initiative acts with greater uncertainty. This uncertainty increases the likelihood of disorientation and an ineffective defense.

This discussion of initiative raises another determinant of advantage in strategy that Clausewitz calls *coup d'oeil*, which we might call insight. Clausewitz did not specifically include *coup d'oeil* in his list of determinants of advantage, but he clearly recognized the importance of *coup d'oeil* to the conduct of war. Clausewitz himself argued that *On War*'s purpose is to help its readers develop *coup d'oeil*.[13] Military and air power theorist, Colonel John Boyd, conceptualized *coup d'oeil* as orientation. Orientation is the interactive process of implicit cross-referencing of intelligence, experience, and predilections that shapes one's perception of patterns in the world.[14] Because war is complex – composed of volatility, uncertainty, chance, and ambiguity – one's perception of patterns in the world will always be an approximation of reality.[15] Consequently, at best one will always be disoriented to some degree. Furthermore,

---

[10] Michael Howard and Peter Paret as cited in Clausewitz, *On War*, 363. The German term translated into "initiative" is *Uberfall*, which literally means to surprise attack.

[11] Clausewitz, *On War*, 198.

[12] Clausewitz, *On War*, 406.

[13] Clausewitz, *On War*, 100-112, 141. Clausewitz spends an entire chapter on the value of military genius and *coup d'oeil* as an element of genius. Clausewitz later goes on to state, "Theory the becomes a guide to anyone who wants to learn about war from books; it will light his way, ease his progress, train his judgment, and help him to avoid pitfalls…[Theory] is meant to educate the mind of the future commander, or , more accurately, to guide him in his self-education[.]"

[14] Boyd, "Organic Design for Command and Control," 15-16.

[15] Harry R. Yarger, *Strategy and the National Security Professional: Strategic Thinking and Strategy Formulation in the 21st Century* (Westport, CT: Praeger Security International, 2008), 28. The strategic environment in general (which thus includes war) is always marked by volatility, uncertainty, complexity, and ambiguity that results in greater or lesser chaos.

orientation shapes the way one uses the initiative.[16] However, if one is so disoriented that one uses the initiative advantage to take actions that do not contribute to achieving the objective, the initiative is worthless. Therefore, the value of the initiative is determined by one's orientation. Hence, there are seven determinants of advantage in strategy – orientation (*coup d'oeil*), initiative, terrain, concentric attack, the presence of fortresses, popular support, and the exploitation of moral forces.

Initiative in general slightly favors the attacker, as he can strike anywhere along the line of defense in full strength, so there is defensive uncertainty with respect to the anticipated strike.[17] On the other hand, the defense can constantly surprise the opponent with the strength and direction of counterattack.[18] However, the defense alone typically benefits from terrain as it presents obstacles to attack, as well as provides defensive concealment.[19] Such obstacles afford more time, and thus opportunity for the defense to observe the enemy and better prepare, reducing or eliminating the attacker's advantage of initiative.[20] Furthermore, the concealment offered to the defense by terrain means the attacker meets the defense with uncertainty as to the character of defense about to be engaged, further weakening the attacker's initiative advantage.[21]

Unless the defense's speed of intelligence is much greater than the speed of attack, the initiative and advantage of surprise will firmly rest with the attacker. In other words, the chance of surprise for an attack is as the speed of intelligence to the speed of the defense's preparation.[22] The speed of preparation and the speed of intelligence are determined by the relative capabilities between two forces in speed of movement, speed of information transmission, mobility, concealment, and observation. If one side has the advantages of greater movement speed, superior mobility, and better intelligence (derived from the speed of information transmission, as well as the resultant of concealment of

---

[16] Boyd, "Organic Design for Command and Control," 16.
[17] Clausewitz, *On War*, 360.
[18] Clausewitz, *On War*, 360..
[19] Clausewitz, *On War*, 360.
[20] Clausewitz, *On War*, 361. The attackers must approach on roads and paths on which it can be easily observed.
[21] Clausewitz, *On War*, 361.
[22] Corbett, *Some Principles of Maritime Strategy*, 259. This is another formulation of Clausewitz's observation that the initiative depends on speed and secrecy (or the speed of preparation). Clausewitz, *On War*, 198.

one's self from the enemy and observation of the enemy), that force will generally have the advantage of the initiative.

Fortresses, as artificial terrain, provide similar effects with respect to initiative. Additionally, fortresses affect another element of strategic advantage, strength. In a theater of operations, fortresses serve as a base for expeditionary forces to exert control over the countryside, and to weaken the enemy's attack in times of war.[23] The defensive purpose of fortresses is to force the enemy to invest them, thereby weakening the attack.[24] Fortifications weaken an attack in two ways – by forcing the enemy to lay siege to them, which requires the attacker to proceed on his march with fewer forces than he would otherwise, and by attritting enemy forces through battle. Therefore, fortresses help bring the enemy to culmination such that as the attack progresses deeper into the theater, the balance of strength eventually changes to favor the defender. At that point, the defense can mount a successful counterattack. If the attacker did not lay siege to the fortresses, he would be vulnerable to flank attacks on his lines of communications launched by expeditionary forces flowing from the bypassed fortresses.

The advantage of concentric attack is also one of strength. Concentric attack brings the double effect of concentrated fire on the enemy and the threat of cutting off the defender's retreat, inducing fear.[25] In practice though, a flanking attack is generally more effective because there is typically an element of uncertainty regarding defensive positions and disposition that make the dispersal of force for encirclement too risky for the attacker.[26] Exterior lines make it difficult for attacking units to render mutual support in the event the defense can seize the initiative, thereby increasing the risk of attempting an encirclement. The defense also enjoys the advantage of interior lines given their concentration of forces being closer together.[27] This lets the defense achieve local concentrations of force through mutual support and use concentric counterattack locally to offset the attacker's advantage of convergent lines of assault.[28] The defense, assuming

---

[23] Clausewitz, *On War*, 394,497.
[24] Clausewitz, *On War*, 407,497.
[25] Clausewitz, *On War*, 360.
[26] Clausewitz, *On War*, 531.
[27] Clausewitz, *On War*, 368.
[28] Clausewitz, *On War*, 360-61.

it embraces the principle of movement, can take advantage of its interior lines to alter its form, its relative dispersion and concentration of forces, more rapidly than the attacker who must move on exterior lines. The advantages and disadvantages of convergent and divergent attack explained by Clausewitz are actually special cases of the more general principles of concentration and dispersion.

Ideally, units of a military force are dispersed enough such that a large part of the force cannot be encircled and destroyed by a single blow.[29] Simultaneously, the units should be near enough to render mutual support to prevent defeat in detail, as well as to concentrate the entire force at the time and place of attack.[30] Notice there is no distinction between defense and attack, or exterior and interior lines regarding the concepts of concentration and dispersion. Whether a military force has balanced its disposition effectively between concentration and dispersion depends on the speed, mobility, intelligence, and protective capabilities of the individual units, in addition to the organization, doctrine, training, skill, and morale of its personnel. The relative capabilities between two forces to concentrate and disperse – in turn based on their relative qualities of speed, mobility, intelligence, and protection – determine which belligerent enjoys the relative advantage in concentric attack.

[29] Corbett, *Some Principles of Maritime Strategy*, 152.

[30] Corbett, *Some Principles of Maritime Strategy*, 132. The object of naval concentration is to cover the widest possible area while preserving elastic cohesion, so as to secure rapid condensations of any two or more of the parts, and in any part of the covered area at will; and above all, ensure a rapid condensation of the whole at the strategical center.

CHAPTER 2

THE CYBER BATTLESPACE

The Conventional Wisdom

A review of official US strategy and doctrine yields little insight into how the US military envisions the use of cyber power in war. Additionally, to the extent that the US military defines the characteristics of the cyber battlespace, it does so in a cursory fashion. Furthermore, the majority of documents uncritically state that cyber attack holds the advantage over cyber defense without analyzing how the nature of cyberspace relates to the accepted determinants of strategic advantage – orientation, initiative, terrain, concentric fires, fortresses, popular support, and moral factors.[1] A brief summary of the pertinent elements from US strategy and doctrine describing the American military view of the cyber battlespace follows.

The Quadrennial Defense Review

To illustrate, the 2010 *Quadrennial Defense Review* (QDR) identifies the need for strategies and policies to improve defense-in-depth of cyberspace, to improve network resiliency, and to provide surety of data and communications in order to facilitate continued confidence in the use of cyberspace during times of conflict.[2] To accomplish this, the QDR states that the Department of Defense (DOD) culture and organization are central to the effort.[3] The document also calls for development of new operational concepts, such as dynamic network defense.[4] For all the focus the QDR places on the development of defenses, the document states without rationale that speed and anonymity of cyber attack *greatly* favor the offense.[5] Additionally, the DOD sees the cyber attack advantage over defense growing as cyber attack tools become cheaper and easier to

---

[1] Clausewitz, *On War*, 363.
[2] Department of Defense, *Quadrennial Defense Review* (Washington, DC: 2010), 38.
[3] Department of Defense, *Quadrennial Defense Review*, 38.
[4] Department of Defense, *Quadrennial Defense Review*, 38.
[5] Department of Defense, *Quadrennial Defense Review*, 37.

employ.[6] As a result, the QDR envisions an environment where only constant vigilance combined with preparation to react almost instantaneously to a cyber attack will allow a cyber defender to effectively limit damage from the most sophisticated attacks.[7]

The National Military Strategy

The United States' 2011 *National Military Strategy* (NMS) provides a little more detail about the US military view of cyber power in war than the QDR. The NMS rightly differentiates cyberspace, a globally connected domain, from the global commons of sea and space.[8] As a globally connected domain, the document states that cyberspace has become simultaneously more critical to military operations and more vulnerable to cyber attack.[9] Regarding the threat, the NMS, similar to the QDR, highlights a persistent, widespread, and growing hostile environment in cyberspace.[10] Given this threat, the NMS calls for a growth in capabilities that will allow the US military to be resilient as a force should cyberspace be rendered unusable or inaccessible.[11] To mitigate the threat, the document directs US Cyber Command (USCYBERCOM) to collaborate with other entities on cyber norms, as well as improve cyber situational awareness and provide a broad range of options to ensure access to cyberspace, as well as hold cyber attackers accountable.[12] More specifically, the NMS states that the joint force will secure the *.mil* network domain, which requires a resilient network architecture that employs a combination of detection, deterrence, denial, and multi-layered defense.[13] In short, the NMS states that the US military will secure cyberspace using defense-in-depth and resiliency in a hostile environment.

---

[6] Department of Defense, *Quadrennial Defense Review*, 37..

[7] Department of Defense, *Quadrennial Defense Review*, 37.

[8] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: Redefining America's Military Leadership* (Washington, DC: 2011), 3.

[9] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: Redefining America's Military Leadership*, 3.

[10] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: Redefining America's Military Leadership*, 9.

[11] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: Redefining America's Military Leadership*, 9.

[12] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: Redefining America's Military Leadership*, 10.

[13] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: Redefining America's Military Leadership*, 19.

The National Military Strategy for Cyberspace Operations

In support of the higher level QDR and NMS, the 2006 *National Military Strategy for Cyberspace Operations* is the first document to identify what the DOD considers cyberspace's key features. These features are:

1) *Man-Made Domain*
2) *Technical Innovation* – Keeping pace with innovation in cyberspace requires sustained and constant vigilance, as well as a high degree of cyber expertise.
3) *Volatility* – Constant change in the domain makes some targets transitory and offense and defense operations challenging. For example, a previously vulnerable target might be replaced or provided with new defenses without warning.
4) *Information Movement* – Lack of geopolitical boundaries allows cyber operations to occur rapidly, nearly anywhere.
5) *Speed* – The speed of information movement approaches the speed of light. This speed can be a source of combat power as it affords commanders the opportunity to make more rapid decisions. However, speed can degrade cyber operations by triggering unintended detection and evasion by an adversary.[14]

Regarding these features, the document implies that the character of cyberspace favors the offense because the current architecture of cyberspace is permissive to malicious activity. Additionally, cyberspace's architecture is such that actions intended to be local in scope can rapidly become global in effect.[15] In making this statement, the document suggests that by changing the man-made architecture of cyberspace, the dynamic between cyber attack and cyber defense can be changed to favor the defense. However, the NMS-CO appears to contradict this implication when it states that technical vulnerabilities are inherent in cyber operations.[16] If vulnerabilities are inherent, they are part of the nature of cyberspace and no change to cyberspace's architecture will alleviate them; such actions could, at best, only mitigate vulnerabilities. This suggests that the authors of the NMS-CO share the conviction expressed in the QDR and NMS, that cyber power favors attack over defense. Furthermore, this document is the first US strategy document to

---

[15] Department of Department of Defense, *The National Military Strategy for Cyberspace Operations* (Washington, DC: 2006), D-1. Document is now declassified.

[16] Department of Defense, *The National Military Strategy for Cyberspace Operations*, D-1.

recognize that cyberspace is multi-layered, stating that cyberspace is best understood as relating to the physical and information dimensions of the information environment.[17]

Lastly, the NMS-CO is the first document to mention any of the determinants of strategic advantage, the initiative, in the cyber context. The document highlights gaining and maintaining the initiative to operate within adversary decision cycles as the number one strategic priority.[18] Unfortunately, this comment also reflects an incomplete understanding of the adaptive capacity that cyber power brings to a military force as a source of harmony, variety, and rapidity in the complex war environment where only the fittest thrive.

Joint Doctrine for Information Operations

Unlike the higher level documents, Joint Publication (JP) 3-13 *Information Operations* does not address cyberspace directly. Instead, the publication divides the information environment into three dimensions: the physical, informational, and cognitive.[19] For the purposes of this thesis, cyberspace is defined as a domain within the information environment whose distinctive characteristics are framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communications technologies.[20] This definition roughly corresponds to the informational dimension described in JP 3-13 as the arena "where information is collected, processed, stored, disseminated, displayed, and protected."[21] The informational dimension consists of information content and flow.[22] By excluding cyberspace from this document, JP 3-13 demonstrates that it is clearly out of sync with higher level US military strategy and policy.

JP 3-13 describes 11 actions that information operations (IO), and thus cyber power, are useful to accomplish: destroy, disrupt, degrade, deny, deceive, exploit,

[17] Department of Defense, *The National Military Strategy for Cyberspace Operations*, 5.
[18] Department of Defense, *The National Military Strategy for Cyberspace Operations*, 19.
[19] Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006, I-2.
[20] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.
[21] JP 3-13, *Information Operations*, I-2.
[22] JP 3-13, *Information Operations*, I-2.

influence, protect, detect, restore, and respond.[23] The document describes these actions without considering the impact of dynamic interaction with a thinking opponent; it thus fails to describe how these actionss help US forces create positions of advantage in the information environment. The publication appears to assume all these tasks will be performed in support of the overall military operation. To a large degree, JP 3-13 apparently assumes an advantage in cyber power, assuming information/cyber superiority, without explaining how the inherent characteristics of cyber power interact to produce superiority in cyberspace, which contributes to overall military advantage.

Another limitation of JP 3-13 is that it considers cyber power to be concerned primarily with affecting adversary decisions and decision-making processes while defending friendly decision-making processes.[24] JP 3-13 clearly fails to recognize that the continued integration of cyberspace into ever more military hardware increases the potential to generate physical combat effects, to disable or disrupt traditional combat systems. For example, it is now possible to disable some automobiles remotely by cyber attack.[25]

Although JP 3-13 does not recognize the increasing ability of cyber power to produce effects beyond an enemy's decision cycle, the document elevates the importance of intelligence in support of cyber power. In doing so, the publication brings to light that the complexity of cyberspace often requires long lead times to generate the intelligence required for effective cyber operations.[26] Regardless, JP 3-13 does not offer significant insight into the distinctive nature of the cyber battlespace, or into how the nature of that battlespace affects the ability to gain a relative cyber power advantage in war.

Air Force Doctrine for Cyberspace Operations

In contrast to JP 3-13, Air Force Doctrine Document (AFDD) 3-12 *Cyberspace Operations* does offer a partial insight into how one of the determinants of strategic

---

[23] JP 3-13, *Information Operations*, I-9-I-10.

[24] JP 3-13, *Information Operations*, I-6.

[25] Karl Koscher et al., "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*, 16-19 May 2010, (Oakland, CA: Center for Automotive Embedded Systems Security, 2010), http://www.autosec.org/pubs/cars-oakland2010.pdf (accessed 31 May 2011), 4. Kevin Poulsen, "Hacker Disables More Than 100 Cars Remotely," *Wired*, 17 March 2010, http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/ (accessed 27 May 2011).

[26] JP 3-13, *Information Operations*, III-4.

advantage Clausewitz identified, concentric attack, translates into cyber power through a brief explanation of one facet of cyber mobility. Notably, AFDD 3-12 describes the concept of logical maneuver.[27] In cyberspace, defense against hostile entry resides in the computer logic code of host systems.[28] As a result, code writing is a form of logical maneuver.[29] Aside from this new concept, AFDD 3-12 is unsubstantially different in its discussion of cyber power from other military publications. Like JP 3-13, AFDD 3-12 provides few explanations of how to translate cyber power capabilities into a warfighting advantage.

National Security Agency Defense-in-Depth Information Assurance Strategy

In 2001, the National Security Agency (NSA) published an information assurance strategy to guide cyber defense implementation. The strategy recommends a defense approach captured by the phrase, "Protect, Detect, React."[30] The strategy stated that cyber defenders should expect attacks, and include attack detection tools that allow the defense to react and recover.[31] The strategy is based on several principles. The first principle is to defend in multiple places within cyberspace.[32] At a minimum, the strategy recommends that cyber defense should focus on the following places: the network and infrastructure, the enclave boundaries using firewalls and intrusion detection, and the computing hosts, servers, and computers.[33] Layered cyber defenses are necessary, according to the document, because the best cyber security products still have inherent weaknesses an enemy can exploit with time.[34] Therefore, each defensive layer should present a unique obstacle, incorporating protection and detection, to an attacker that helps increase an enemy's risk of detection while decreasing his probability of success.[35] Lastly, cyber defenders should design their defensive cyber infrastructure to help answer

[27] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 15 July 2010, 3.
[28] AFDD 3-12, *Cyberspace Operations*, 3.
[29] AFDD 3-12, *Cyberspace Operations*, 3.
[30] National Security Agency, *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments*, 8 June 2001, http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed 2 March 2011), 1.
[31] National Security Agency, *Defense in Depth*, 1.
[32] National Security Agency, *Defense in Depth*, 2.
[33] National Security Agency, *Defense in Depth*, 2.
[34] National Security Agency, *Defense in Depth*, 3.
[35] National Security Agency, *Defense in Depth*, 3.

the questions: "Am I under attack? Who is the source? What is the target? Who else is under attack? What are my options?"[36]

Since the NSA published this cyber defense strategy in 2001, the character of cyberspace has changed according to the Technical Director of the NSA's Systems and Network Analysis Center, Trent Pitsenbarger. Defending the enclave has become less important as the character of cyberspace has become more porous and architectures like cloud computing spread.[37] As a result, the NSA is placing more emphasis on policy based defenses like controlling user privileges within a network, than using enclaves and firewalls to control user access to a network.[38] This shift in emphasis is part of a new NSA and US Cyber Command cyber defense paradigm called active defense.

Active cyber defense is dynamic, tailored for each network, and team based; it develops countermeasures to thwart an adversary as he adapts.[39] Active cyber defense uses sensors and maps to detect intrusions.[40] Active defense employs warning from intelligence capabilities to deploy defenses and counter intrusions in real-time.[41] For the *.mil* region of cyberspace, active defense places scanning technology at the interface of military networks and the Internet.[42] Because of the speed inherent to cyberspace, political leaders and military commanders must set rules of engagement for active cyber defenses in advance.[43]

Active cyber defense refines, and adds detail to, the Protect, Detect, React model that the NSA described in 2001. The major refinement is the incorporation of

---

[36] National Security Agency, *Defense in Depth*, 3.

[37] Trent Pitsenbarger (Technical Directory, Systems and Network Analysis Center, National Security Agency), interview by author, 2 May 2011. Eric Knorr and Galen Gruman, "What cloud computing really means: The next big trend sounds nebulous, but it's not so fuzzy when you view the value proposition from the perspective of IT professionals," *InfoWorld*, 7 April 2008, http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 (accessed 27 May 2011). "Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities."

[38] Pitsenbarger, interview by author.

[39] GEN Keith Alexander, Commander, US Cyber Command (address, RSA Conference 2011, San Francisco, CA, 17 February 2011), http://media.omediaweb.com/rsa2011/keynotes/webcast.htm?id=3-1 (accessed 10 May 2011).

[40] William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberspace Strategy," *Foreign Affairs* 89, no. 5 (2010): 103.

[41] Lynn, "Defending a New Domain: The Pentagon's Cyberspace Strategy," 103.

[42] Lynn, "Defending a New Domain: The Pentagon's Cyberspace Strategy," 103.

[43] Lynn, "Defending a New Domain: The Pentagon's Cyberspace Strategy," 103.

intelligence warning into the model so that the defense can react more quickly. Detection is still a critical component of cyber defense in the active model.

Although these models do not use traditional military language to describe the elements of cyber defense, their strategies do rely on those concepts. For example, by using intelligence warning to deploy real-time countermeasures, the defense assumes the initiative advantage relative to attack. Additionally, the questions identified for a cyber defense infrastructure to answer highlight a tacit recognition of the orientation concept. The NSA deserves credit for incorporating traditional military strategy concepts into their cyber defense strategy. However, the non-use of traditional military language when describing these concepts suggests that these ideas were invented anew, not adapted from knowledge of military strategy on attack and defense. Understanding cyberspace's character and how it shapes the application of military strategic concepts is essential to incorporating cyber power into joint military operations.

Distinctive Characteristics of the Cyberspace Warfighting Domain

A military force's fitness, its ability to adapt in the chance-laden environment of war, depends on the qualities of variety, rapidity, harmony, and initiative the force possesses.[44] Clearly rapidity, speed of action, is one characteristic that distinguishes cyberspace from the other warfighting domains. Cyberspace is a domain within the information environment whose distinctive characteristics are framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks of hardware and/or software at all levels from the integrated circuit, to the central processing unit, to the personal computer, to the Internet.[45] In cyberspace, actions occur at machine speeds, speeds approaching the speed of light. Unlike the physical domains, which largely rely on observation means (radar, signals intercepts, electro-optical-infrared sensors) that collect and generate information near the speed of light to detect actions occurring at much, much, slower speeds; observation and action speeds have a small differential, if any, in cyberspace. As described previously, unless the defense's speed of observation is

[44] Boyd, "Patterns," 11-12.
[45] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.

much greater than its speed of action, the initiative and advantage of surprise firmly rest with the attacker.[46] As a result, absent knowledge before an engagement begins by either side about how, what, where, and when a cyber attack or defense will be conducted, a cyber attacker will enjoy the advantage of surprise achievable in other domains only with the aid of deception or concealment.

The ability for surprise is governed by the differential between the speed of observation and the speed of action. The greater this differential in favor of the speed of observation, the greater the temporal depth a defender enjoys, decreasing the attacker's normal advantage of initiative. However, temporal depth in the physical domains is not a pure function of the ratio between the speed of observation and the speed of action. For example, a defending soldier standing in low ground with binoculars cannot see as far as a soldier standing on a hill. For both soldiers, the speed of intelligence is the same, but they do not share the same temporal defensive depth due to their vantage points. Vantage and, as a corollary, mobility therefore affect temporal depth.

In combat, one needs to resolve several parameters to effectively engage an enemy – its position in three-dimensions, its speed, and its direction of travel. To engage a target, one needs to know where it is, and where it will be. This problem is simplified if the target has relatively less mobility (i.e. can only travel in one direction, or can only change direction slowly). For example, an aircraft has greater mobility than a surface ship because an aircraft can maneuver in all three-dimensions vice two, as well as change its position in space and its direction of travel far more quickly than a ship. These properties make completing the kill chain a simpler problem against a surface ship target compared to an aircraft target. A target's vertical, longitudinal, and lateral position, its speed, and its direction of travel represent what might be called in engineering terms the degrees of freedom in the targeting problem. There are five degrees of freedom in the targeting problem for the physical warfighting domains of land, sea, air, and space. The ability to change these five variables, and the speed with which these variables can change, describe mobility in these domains.

46 Corbett, *Some Principles of Maritime Strategy*, 259.

A distinctive characteristic of cyberspace is that there are more than five degrees of freedom governing the targeting problem – there are nine, but not all need be known to successfully engage a target depending on whether one intends to engage a cyber target using kinetic or cyber means. The additional four variables arise from the fact that cyberspace, unlike the other domains, is synthetic. Cyberspace is man-made and resultantly reparable and alterable.[47] Consequently, a cyber target has both a physical location as well as an artificial, virtual location – the first degree of freedom derived from cyberspace's synthetic nature. Currently, the virtual location in cyberspace is typically described by a single value, an object's internet protocol (IP) address. However, because cyberspace is artificial, the number of values associated with a target's virtual location is theoretically unlimited, implying that the number of degrees of freedom governing a cyberspace targeting problem is not fixed at nine, but could increase.

In addition to a target's virtual location, cyberspace's synthetic nature gives rise to what AFDD 3-12 terms logical maneuver space.[48] The syntactic layer of cyberspace reflects the format of information, how information systems function, and how those systems are manipulated.[49] The very rules that define the boundary conditions for action in cyberspace are variable and exploitable. The speed of action in cyberspace allows these rules to be reconfigured rapidly, creating another degree of freedom. By manipulating the rules, one can alter how commands in cyberspace are interpreted into action, whether on attack or defense. No analog exists to this form of mobility in the physical domains. In the world of Newtonian physics, for every action, there is a predictable, equal and opposite reaction. Based on Newtonian principles, tanks move, ships sail, aircraft fly, and satellites orbit. The laws governing action in cyberspace are not completely universal, much of how any particular information system interprets commands is customizable, and therefore inherently uncertain *a priori*.

---

[47] Libicki, *Conquest in Cyberspace*, 5. Cyberspace is replicable and therefore reparable.

[48] AFDD 3-12, *Cyberspace Operations*, 3.

[49] Libicki, *Conquest in Cyberspace*, 8-10. Cyberspace consists of three layers. The physical layer – the wires, routers, etc. – is the foundation of cyberspace in the tangible world. The syntactic layer reflects information format, as well as how information systems that form cyberspace are instructed and controlled. The semantic layer is where information meaningful to humans resides.

In addition, the synthetic nature of cyberspace affects the number of directions of travel. As Julian Corbett observed for the sea, the number of possible paths between any two ports is nearly infinite because transportation on the open seas is largely unimpeded by terrain features.[50] A similar situation holds in the air. However on land, terrain features often limit avenues of approach. Cyberspace's synthetic nature implies two more degrees of freedom, the numbers of physical and virtual paths between two points, which are simultaneously finite and infinite. The physical and virtual directions of attack are possibly infinite because new physical and virtual paths can be rapidly created or destroyed.

Thus, the four additional degrees of freedom describing mobility in cyberspace arising from its synthetic nature are: virtual location, customizable rules of action, customizable physical pathways, and customizable virtual pathways. Unlike the physical domains where the character of any battlefield, its geography and terrain, is largely a given to both belligerents, the character of the battlefield in the cyber domain is an element that each side manipulates. The additional degrees of freedom in cyberspace are a source of variety. However, this fact leads to an additional level of complexity, the consequence of which is that specific effects of cyber attack on the enemy tend to be indirect and unpredictable.[51]

There also exists a quality of concealment arising from cyberspace's nature. Cyberspace simply is not a domain into which humans can physically enter, making it easier to conceal one's activities. Unlike in the other domains where people can directly observe and therefore simultaneously observe cause and effect, one can often only initially observe the effect of an adversary's actions in cyberspace. A similar dynamic is observed in particle physics captured by the Heisenberg uncertainty principle, which

[50] Corbett, *Some Principles of Maritime Strategy*, 158-59. Afloat, neither roads nor obstacles exist. Practically nothing limits freedom of movement on the sea except the exigencies of fuel.

[51] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 19-20. The indirect effects of a cyber attack are almost always more consequential than the direct effects. This is because the individual computers attacked are often far less important than the system(s) controlled by the targeted computers or the decision-making that depends on the information in, or processed by, the targeted machines. The outcomes of cyber attack are often highly uncertain because minute configuration details can affect the result, and cascading effects frequently cannot be predicted reliably.

states that one cannot know both the position and velocity of a sub-atomic particle.[52] The principle arises from the fact that any attempt to accurately measure the location of a particle will disturb the particle's trajectory, and thus its velocity, while any attempt to measure the velocity of the particle leaving its trajectory undisturbed implies that one can only confine the particle's location to a region. Furthermore, particle physics measurements are made indirectly. Velocity and position measurements are made by observing disturbances in electromagnetic fields as particles pass through them, not by directly observing the particles themselves.[53] Scientists know the particles are there because of the disturbance to the natural order, the effect, observed. Thus, there will always be a probabilistic element to particle physics measurements that arises from the reality that observations of particle existence are necessarily indirect. Cyberspace's complex nature (composed of nested, interdependent networks) dictates that effects of actions in cyberspace are indirect and can have multiple causes.[54] So in many respects, attribution of causation is also inherently probabilistic, which makes adversary penetration of, and to a lesser degree action within or against, friendly cyberspace more difficult to identify and naturally more concealable.

Cyberspace's complexity derived from its nature of nested, interdependent networks facilitates concealment, as well as harmony and disharmony. The networked, interdependent nature of cyberspace allows its elements to self-regulate (negative feedback) and remain in harmony with each other. Cyberspace's networked nature also allows effects at one network node to perpetuate through the system rapidly (positive feedback). Unfortunately, this positive feedback can be either beneficial, or detrimental

[52] Public Broadcasting Station, "People and Discoveries: Heisenberg states the uncertainty principle, 1927," *A Science Odyssey*, http://www.pbs.org/wgbh/aso/databank/entries/dp27un.html (accessed 27 May 2011). "[T]he act of observing alters the reality being observed. At least at the subatomic level. To measure the properties of a particle such as an electron, one needs to use a measuring device, usually light or radiation. But the energy in this radiation affects the particle being observed. If you adjust the light beam to accurately measure position, you need a short-wavelength, high-energy beam. It would tell you position, but its energy would throw off the momentum of the particle. Then, if you adjust the beam to a longer wavelength and lower energy, you could more closely measure momentum, but position would be inaccurate."

[53] Public Broadcasting Station, "People and Discoveries: Heisenberg states the uncertainty principle, 1927." Particle measurements are made by observing disturbances in beams of light, also known as an electromagnetic field.

[54] Libicki, *Conquest in Cyberspace*, 41. "The effects of attacks in cyberspace are often hard to distinguish from mistake or accident."

and lead to disharmony. These positive feedback effects are frequently referred to as cascading effects. Through cascading effects, cyberspace's networked nature can be a source of rapidity for adaptation, but also a source of rapid, unpredictable system collapse.

Lastly, cyber power has a natural element of persistence, meaning the cause of hostile cyber effects can persist until action to negate them is taken. Cyberspace is an information storage medium by definition.[55] Information storage has no utility if that storage is fleeting and information can disappear without deliberate deletion. It is this property of information storage that permits automation of action, because computer instructions, computer command and control, persist as a result. The natural consequence of information storage as a fundamental aspect of cyberspace is that the causes of effects in cyberspace tend to persist, and thus too the effects themselves tend to persist, absent deliberate action to the contrary. As a result, cyber actions do not require continuous effort to produce continuous effect in many instances. Additionally, persistence eases one's ability to conceal cyber power because, for example, a cyber logic bomb theoretically could lie dormant indefinitely until an attacker chooses to unleash it in a surprise attack.[56] Furthermore, automation creates a disconnect between action and human actor, much like a letter bomb. One might be able to trace an action to a specific machine, like the post office a letter bomb was sent from based on the postmark, but linking the malicious act to a human perpetrator is far more difficult. Consequently, the cyberspace property of information storage, which results in persistence, is also a source of concealment for the human actor. Furthermore, persistence combined with concealment facilitates not just attacks on an enemy's center, but like sabotage, concealment facilitates attacks emanating from within the enemy's center.

In summary, cyberspace's distinguishing features are: near parity between speed of action and speed of observation because all actions occur near the speed of light, more complex mobility derived from cyberspace's synthetic nature, observational uncertainty

---

[55] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.

[56] *Merriam-Webster's Dictionary*, n. "logic bomb," (2011), http://www.merriam-webster.com/dictionary/logic%20bomb (accessed 27 May 2011). A logic bomb is "a computer program often hidden within another seemingly innocuous program that is designed to perform usually malicious actions (as deleting files) when certain conditions have been met."

easing concealment, networking permitting greater potential for rapid adaptation or rapid collapse, and persistence of causation. These features combine to form the distinctive nature of the cyberspace warfighting domain.

Cyber Attack and Cyber Defense

There are seven primary determinants of advantage in strategy between attack and defense in the physical world. The same seven factors primarily determine advantage in strategy between attack and defense in cyberspace: orientation, surprise and initiative, terrain, concentric fires, fortifications, popular support, and moral factors. In this warfighting domain, cyber attack is the use of cyber power to alter, disrupt, deceive, degrade, or destroy adversary computer systems and networks, or the information and programs resident in, or transiting through, cyberspace.[57] Cyber defense comprises those actions taken in order to preserve one's cyber power, to preserve one's ability to exploit cyberspace for advantage.[58]

Cyberspace resides simultaneously, physically and virtually, within and outside geographic boundaries.[59] Computers, wires, routers, switches, and so on comprise the physical portion of cyberspace.[60] Cyberspace's virtual existence arises from its syntactic and semantic layers.[61] The syntactic layer of cyberspace reflects the format of information, and how the information systems forming the physical layer of cyberspace are instructed and controlled.[62] The semantic layer contains the information meaningful to humans, the element of cyberspace at the human-machine interface.[63] From cyberspace's characteristic of physical and virtual existence arises the cyber analog to terrain in the land domain.

Land Power Analogs to Cyber Power – Terrain and Fortresses

Cyberspace has features analogous to terrain in the land domain arising from its physical existence. Like land, cyberspace exists as a set of non-contiguous entities

[57] Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 10.
[58] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.
[59] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.
[60] Libicki, *Conquest in Cyberspace*, 8.
[61] Libicki, *Conquest in Cyberspace*, 8-10.
[62] Libicki, *Conquest in Cyberspace*, 8.
[63] Libicki, *Conquest in Cyberspace*, 9.

varying in size, entities among which one cannot traverse via cyberspace alone. In other words, some elements of cyberspace exist as an interconnected whole, while other portions of cyberspace exist apart from that interconnected whole.[64] These cyberspace "islands" are air-gapped from the global network and cannot be entered without physical access to the hardware that brings these "islands" into being.[65] Some of these "islands" are large, and some are small.[66] Regardless, to use cyber power generated on one "island" in another, one must transport that cyber power across the air-gap by other than cyber power means, just as the United States must transport its land power to other continents using sea and air power. Additionally, there are a finite number of physical paths through which data can transit between any two elements of computer hardware in cyberspace. Because air, space, and the sea are continuous, homogeneous domains, one can approach a destination from essentially any azimuth, along a near infinite number of paths between two points. Cyberspace is not a physically continuous or homogeneous domain like air, space, or much of the sea. Just as in the land domain, a road network exists in cyberspace that is artificial (man-made), reparable, and manipulable to those with physical control of the area. Therefore, information transit between two physical points in cyberspace is more predictable because it is constrained to a finite number of paths, just as the movement of tanks between two towns in a mountainous region is more predictable because it is largely constrained by the road network in the area.

Another cyberspace feature analogous to a feature of the land domain, mountainous terrain, arises from cyberspace's virtual existence, specifically the syntactic layer. The software that forms the syntactic layer of cyberspace is growing ever more complex. So complex that it is virtually impossible to know in advance all of the syntactic entry paths into a portion of cyberspace.[67] In this way, cyberspace resembles mountainous terrain in the land domain. While the number of paths a mechanized army

---

[64] Albert-László Barabási, *Linked : The New Science of Networks* (Cambridge, MA: Perseus Pub., 2002), 167-69. The World Wide Web does not form a homogeneous network. Islands of cyberspace, which one cannot reach from the major portions of the Web, exist. All directed networks exhibit this property.

[65] Libicki, *Conquest in Cyberspace*, 33. Air-gapping is the total electronic separation of networks from the outside.

[66] Barabási, *Linked : The New Science of Networks*, 167-69.

[67] National Security Agency, *Defense in Depth*, 3. Even the best information assurance products have inherent weaknesses so it is only a matter of time before the enemy finds an exploitable vulnerability.

may take between two towns in cyberspace is finite and controllable by the residents of the town, the number of approaches on foot in the vicinity of the town is complex due to the terrain.[68] Given enough time and resources, an attacking army will eventually find an unguarded or lightly guarded approach to the town.[69] Similarly, the complexity of software that makes up the syntactic layer of cyberspace is such that a cyber attacker will eventually find an unguarded or lightly guarded opening through which to gain access to an information system, given enough time and resources.[70]

If cyberspace is analogous to the land domain, then like a sturdy castle, a well-built cyber fortress should be exceptionally strong, giving the defense a battle advantage in strength relative to the offense. Counterintuitively, this is not so. Cyber fortresses typically use "firewalls," access controls to keep attackers out of the defended cyberspace. However, because these cyber fortresses lie in the complex mountainous terrain created by the syntactic layer of cyberspace, cyber attackers with sufficient resources will almost always locate a weakly defended approach to the fortress that their assault can exploit. The nature of cyber power nearly guarantees the availability of such resources. Often a single computer and one individual's intellect, protected by the concealment inherent in cyber power, are all the resources necessary. A fortress in cyberspace is relatively stronger tactically given the finite number of physical approach avenues (wires/electronic links between two points) afforded by the domain's mountainous character. Unfortunately, the same mountainous character results in an overall strategic advantage for the cyber attacker because finding a lightly defended approach is mostly a matter of time for a committed attacker, regardless of the strength of the defender's fortress.

[68] Clausewitz, *On War*, 420. Impassable is often confused with inaccessible in mountain warfare. Where one cannot advance in a column, or with artillery or cavalry, one can still advance with infantry. "The belief that posts enjoy secure communications with each other therefore rests on a complete illusion[.]"

[69] Clausewitz, *On War*, 420. Mountain posts flanked by a ravine/precipice is a good point of support not because it is impossible for the enemy to turn the flank, but because a turning movement burdens the enemy with a cost in time and effort that has to be measured against the posts significance.

[70] Libicki, *Conquest in Cyberspace*, 36. One trend in commercial software is greater complexity, which creates more places for security-undermining error.

Clausewitz identifies another weakness of fortress defensive systems in mountains for land warfare – the inability to provide mutual support.[71] It is difficult for land power to provide mutual support between fortresses in mountains because land power's speed is limited, so reinforcements that must traverse high and low ground are vulnerable as they move to outflank the attacker.[72] However, cyber power's machine speeds are such that the domain's complexity would not unduly expose reinforcements from supporting cyber fortresses. Where Clausewitz cautions against a system of defensive fortresses in complex, mountainous terrain for land warfare, he does so because of land power's speed limitations. The absence of these speed limitations suggests that a system of mutually supporting cyber fortresses would still be a viable defensive strategy, regardless of cyberspace's complex, mountainous character.

The *trace italienne* is one of the strongest fortress types ever. It was developed in the late 1440s by Leon Battista Alberti, an Italian architect.[73] The *trace italienne* proved to be a defensible fortification for more than 200 years.[74] These fortresses took a lot of time and manpower to successfully attack. However, the armies that could be raised during the period were limited in size, so a state fortified with a series of *trace italiennes* could not be defeated in total. Some towns so fortified were virtually impregnable. As a result, the wars of the time were often limited in scope. Armies simply were not large enough to simultaneously lay siege to all of an adversary's fortresses, man all of one's own defensive fortresses, and wage a war of maneuver.[75] To wage an unlimited war without an army of sufficient size to accomplish all of these missions in parallel would have left the attacker vulnerable to counterattack on his homeland, as well as susceptible to flank attack on his lines of communication. The *levee en masse* under Napoleon

---

[71] Clausewitz, *On War*, 419. "In mountains, any movement is slower and more difficult; it takes more time, and if it is made within range of the enemy, it also costs more lives." Clausewitz, *On War*, 421. An assault by concentrated and vastly superior forces on a single point will meet with fierce resistance when measured by the strength of that point; but measured by the strength of the whole defensive force, that resistance is negligible. Once the point has been overcome, the defensive line is pierced and the objective is achieved.

[72] Clausewitz, *On War*, 419.

[73] Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800* (Cambridge, UK: Cambridge University Press, 1996), 8.

[74] Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800*, 9.

[75] Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800*, 24. "The key variable appears to have been the presence or absence of the *trace italienne* in a given area, for where no bastions existed, wars of manoeuvre with smaller armies were still feasible."

altered this dynamic, restoring maneuver to the battlefield and greatly reducing the value of any single fortress for the defense in strategy.

The *levee en masse* meant that an army's size was unconstrained such that an attack force could lay siege to multiple fortresses at once, and still have sufficient strength to simultaneously wage maneuver warfare. The rise of mass armies was made possible by a technological advancement that led to the amateurization of warfare – the musket. Prior to the musket, the long bow provided firepower and the knight was superior on the battlefield. Both archers and knights took long periods of time to train.[76] Knights, furthermore, were expensive to train and equip. The musket, combined with the training innovation of drill, allowed soldiers equipped with good firepower to be trained and fielded rapidly. Cyber power permits a similar amateurization of warfare.

Speed of action, automation, and the ability to self-publish in cyberspace create a similar dynamic to that fostered by the musket in land power. Action in cyberspace occurs at machine speeds approaching the speed of light. As a result, different approach avenues to attack cyber defenses in the syntactic layer can be rapidly tried by an adversary using just one machine simultaneously, or nearly so. When the exponential increase in near-simultaneous attack approaches permitted by innovations such as botnets are considered, then one appreciates that a cyber attacker clearly has the resources to lay siege to multiple cyber fortresses just as the Napoleonic *levee en masse* armies did during

[76] J. F. Guilmartin quoted in Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800*, 17. "Where a few days and a good drill sergeant might suffice to train a reasonably good [musketeer], many years and a whole way of life were needed to produce a competent archer."

the late 1700s and early 1800s.[77] Furthermore, to use cyber power in war requires little training beyond the basic computer skills needed for modern daily life. An experienced cyber warrior need not devote significant time and resources to train additional warriors that can act with great effect. The experienced cyber warrior can create automated tools and use them in a botnet, or make the tools with simple instructions available to the masses by self-publishing on the Internet. Both methods allow one to raise a large cyber force rapidly. As a result, a cyber defense strategy relying on passive and static defense by firewalls and access controls alone, filling in holes when a cyber attack exploits one, is a strategy doomed to fail, just as mass armies of the Napoleonic era rendered a static defense built around the *trace italienne* obsolete.

Given the capability of Napoleonic armies to simultaneously lay siege to a system of fortresses and continue maneuvering with a sizeable force, the defending army was faced with the choice of meeting the attacker in maneuver battle, or face defeat in detail as its fortresses, unable to be reinforced without accepting the risk of maneuver battle, eventually fell. Thus, individual fortresses no longer served as sufficient protection for a state during the time of Napoleon, only a system of fortresses capable of mutual reinforcement through maneuver among them significantly increased the strength of the defense. The purpose of the fortress in defense in the Napoleonic era became to weaken the attack by forcing the enemy to invest the fortress and attritting the enemy to bring him to culmination more quickly, as well as to buy time for reinforcements to arrive.

---

[77] Audrey Kurth Cronin, "Cyber-Mobilization: The New *Levee en Masse*," *Parameters* 36, no. 2 (Summer 2006): 77-87. Cronin also makes the analogy between cyber power and the *levee en masse*. However, she focuses on the ability to inspire mass groups and rapidly mobilize them into action. She accurately described inspirational capability of cyber power, but she failed to address how the amateurization of warfare made possible *militarily advantageous* mass mobilization, which is at the center of my use of the *levee en masse*-cyber power analogy. Microsoft, "What is a botnet?," *Safety & Security Center: Computer Security, Digital Privacy, and Online Safety*, http://www.microsoft.com/security/resources/botnet-whatis.aspx (accessed 27 May 2011). "The term bot is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, your computer might slow down and you might inadvertently be helping criminals."

In mountainous terrain, mutual reinforcement among fortresses is difficult. The rugged terrain makes the movement of reinforcing infantry over land slow. The reinforcing troops must transit both peaks and valleys enroute to the fortress while under duress. The advantage of the high ground accrues to the attacker who is stationary and concentrated around the fortress on the mountain peak. Consequently, the attacker can harass approaching reinforcements, further slowing their movements. Where the attacker has time on his side, the defender with forces under duress does not. In mountainous terrain, attacking siege forces can continue to probe until a weakness is found with even less fear that reinforcements will be able to effectively outflank them, cut them off and defeat them in battle. Cyberspace's complexity, its mountainous character, suggests that the dynamics of cyber attack and defense will exhibit behavior similar to the land power dynamics of attack and defense of fortresses in mountains, with the attacker holding the advantage.

However, the land power analogy to mountainous terrain is not complete for cyber power – speed of action approaches the speed of light for both the cyber attacker and defender. In addition, because cyberspace is man-made, the fact that the speed of cyber reinforcement is slow is artificial, a function of the defensive doctrine adopted vice a limitation inherent to the cyberspace domain. Consequently, reinforcements in cyberspace can move rapidly, unlike infantry in mountainous terrain, and the concept of mobility to outflank an attacker can be used in cyber defense regardless of cyberspace's mountainous character. Despite the complex nature of cyberspace, speed of action in the domain implies that cyber fortresses can and should function for defenders in much the same way they do in land warfare in areas of relatively easy movement.

Sea Power Analogs to Cyber Power – Intelligence and Persistence

Like with the land domain, cyberspace also shares several characteristics with the sea domain. Both are domains across which commerce travels. The distribution of cyberspace is comparable to the distribution of water on the planet, with vast interconnected cyber oceans coexisting with cyber lakes and seas, sometimes connected by cyber rivers, sometimes completely isolated.[78] In warfare though, the key similarity

[78] Barabási, *Linked : The New Science of Networks*, 167-69.

between sea power and cyber power is the ability to deny intelligence to an opponent on (to conceal) one's persistent power. Of course, this similarity refers to sea power provided by the submarine.

Concealment for cyber power derives from the nature of cyberspace, from the fact that it is a domain in which the presence of malicious actors can only be observed indirectly. For sea power, concealment is not inherent in the domain itself, but the quality of concealment becomes exploitable when one takes advantage of the physical impediment to light and sound when one travels submersed in the sea instead of on its surface. The submarine conceals itself by shielding its presence beneath the barrier of the ocean's surface.

The submarine's concealment contributes to several advantages in sea power relative to surface ships. Concealment helps give the advantage of initiative to the submarine because it decreases the ratio of the speed of intelligence to the speed of preparation for surface ships. By changing this ratio, concealment also supports a moral advantage for submarine forces because stealth increases their survivability. Whether attacking, or on the defense counterattacking, one is unlikely to hit what cannot be observed. The ratio of the speed of intelligence to the speed of preparation is low for surface ships against submarines. This low ratio implies that submarines can generally attack surface ships while they are less prepared to parry the blow than if the ships were aware of the submarine's imminent attack. The logical extension is that the surface ships are also less prepared to counterattack. These ships will likely have much less time to complete the kill chain against submarines than they would absent the submarine's concealment, which increases the chance the submarine force will survive such an engagement.

Concealment in sea power, combined with persistence, generates a superior ability to concentrate and disperse that gives the advantage of concentric attack to the submarine relative to surface ships. On the sea, ships move relatively slowly. As a result, it can take hours, or even days for a sea force dispersed over a large area to concentrate at the point of attack. To account for this factor in war, sea forces often travel in relatively concentrated groups – fleets, task forces, or convoys – in order to

realize Corbett's recommendations for force disposition.[79] These groups allow sea forces to readily concentrate for mutual support or a total force engagement in minutes or less while maximizing dispersion for force protection. In an engagement, taking hours or days to concentrate would just be unacceptable. Concealment changes this dynamic. Concealment allows a submarine force to disperse over a much larger area than a surface task force, because with the initiative the submarine force can not only attack, but also *refuse* combat according to its whims.

Concealment combines with persistence to confer a strong advantage to submarines. Persistence of presence permits a submarine to track a surface group while refusing battle until sufficient force concentration is achieved to unleash an attack. Therefore, hours or days become acceptable timelines to concentrate the total force for an attack, while mutual support is largely unnecessary because of the submarine's advantage of initiative and the related survivability that concealment facilitates. Unlike concealment being a property specific to submarines (operating below the surface), persistence is a general property of sea power. Only because persistence and concealment combine in the submarine does it retain the advantage of initiative such that a submarine force can largely choose the time and place of attack, negating the slow speed of sea travel that typically prevents rapid concentration of sea power for a widely dispersed force.

Concealment and persistence function in cyberspace to provide advantages analogous to those of the submarine. Concealment is inherent in the exercise of cyber power, which derives from the uncertainty of observing hostile actions in cyberspace because the only means of detection are indirect. Concealment allows hostile cyber actions to be prepared in friendly cyberspace with a low probability of detection, much like a submarine shadowing a convoy while preparing to attack. Also like the submarine, concealment in cyberspace supports an advantage in initiative such that the human actors enjoy increased survivability which yields a moral advantage to hostile actors. Lastly in

[79] Corbett, *Some Principles of Maritime Strategy*, 132. The object of naval concentration is to cover the widest possible area while preserving elastic cohesion, so as to secure rapid condensations of any two or more of the parts, and in any part of the covered area at will; and above all, ensure a rapid condensation of the whole at the strategical center.

combination with concealment, persistence allows those who wield cyber power the advantage of initiative despite the relatively long preparation period required to execute a successful cyber attack driven by cyberspace's complex, mountainous nature.

The long cyber attack preparation period is the similarity beyond which the cyber power analogy to sea power collapses. Fortunately, air power parallels exist to furnish further insight. For instance, the effective use of air power also requires a long period of intelligence preparation.

Air Power Analogs to Cyber Power – Speed, Mobility, and Intelligence

Like the rise of air power before it, cyber power offers a speed of action greatly superior to that possible in any other domain. Also like air power, cyber power possesses the mobility to circumvent an adversary's fielded forces in the other domains and strike at the heart of enemy power from the outset of conflict. However, to effectively and efficiently employ air power extensive intelligence preparation of the battlespace is necessary, often requiring long-lead times.

Air power possessed a speed of action vastly greater than that of land or sea power. Cyber power now offers a similar increase in speed. With activity possible near the speed of light, cyber power's speed of action vastly outstrips the potential for action at the pedestrian speed of sound offered by air power. The dramatic increase in air power's speed of action created a speed ratio of intelligence to preparation for the defense nearly equal to one during the Interwar Years between World Wars I and II. This situation boosted the inherent advantage of initiative already possessed by an attacker such that effective, general air defense was impractical. This dynamic persisted until the invention of radar just prior to World War II, a creation which provided intelligence near the speed of light. Radar reset the speed ratio of intelligence to preparation such that effective, general air defense became practical. The speed ratio changed once again to favor air attack with the initiative advantage with the advent of stealth aircraft in the 1980s. For those possessing stealthy capabilities, the initiative advantage for air attack over defense persists today. Similarly, a speed ratio of intelligence to preparation near unity for cyber power today also favors the attack with superior advantage in initiative and surprise.

Air power's mobility in three dimensions complements air power's speed. This mobility means that an air attack can approach its target from virtually any azimuth and from all, or nearly all, elevations. The resulting multiplicity of approach vectors available to an attacking force greatly complicates the air defense intelligence problem. Air power's mobility results in uncertainty as to the specific target and direction of attack, which increases the inherent initiative and surprise advantage for an air attacker. In addition, air power's mobility in the third dimension allows it to bypass surface defenses, and, due to the ubiquity of the air domain, to hold any physical target at risk. With the ability to simultaneously attack enemy fielded forces and their lines of communication (a classic flank attack), air power's mobility also creates an advantage of concentric attack.

Cyber power's mobility, though cyberspace is not everywhere, creates similar uncertainty for a cyber defender, but with an even greater advantage than air power. Cyber power maneuver has four additional degrees of freedom beyond the air domain.[80] This additional complexity creates an environment of greater uncertainty for the cyber defender, hence more of an initiative advantage for the cyber attacker compared to the advantage held by air attackers. Additional mobility in cyberspace also presents more opportunities to seize the concentric attack advantage. An enemy cyber force can exploit the additional four degrees of freedom in cyber mobility to attack an enemy on multiple virtual fronts as well as multiple physical fronts. The ability to use the degrees of freedom as axes of attack creates more opportunities to outflank one's opponent and a greater ability to employ concentric attack within cyberspace.

Ubiquity of air allows air power to utilize its speed and mobility in order to seize the initiative and concentric attack advantages. Yet, air power is fleeting, although less so in the present than the past. Still, aircraft do not exist in sufficient numbers, with sufficient persistence, to fully alleviate air power's fleeting nature. Because air power is fleeting, an adversary can reconstitute damaged, destroyed, or otherwise negated forces

[80] See section "Distinctive Characteristics of Cyberspace" (page 20 to 23) for a full explanation of the degrees of freedom in cyberspace.

during periods of air power absence. As a result, continuous effort is necessary to make air power's effects persist.[81]

Similarly, cyber power effects persist only with continuous effort. Persistence of cyber power effects requires continuous effort not because cyber power is fleeting, on the contrary persistence is inherent in cyber power, but because cyberspace is rapidly reparable. Rapid reparability in cyberspace makes the effects of cyber power fleeting. Like with air power, the ability for an adversary to repair damage, reparability, drives the need for continuous effort to sustain cyber power effects.

Cyber power in war is about producing effects that contribute to a successful overall joint military campaign. However, the effects that cyber power creates tend to be indirect. This is similarly true for air power. The primary effect of air power on an opponent is disruption, not destruction.[82] This too is in part a consequence of air power's fleeting nature combined with an enemy's ability to repair damage. However, disruption also results because air attack missions, other than close air support, tend to be against elements of enemy systems that are interdependent networks, not discrete, independent entities. Because it is typically infeasible to destroy all elements of an effectively dispersed system against a thinking enemy, air power will typically only be able to target a fraction of the interdependent elements that make up an enemy system. Thus the effects of air power, like cyber power, also tend to be indirect. Enemy target systems, which are networks of interdependent elements, will cease to function at the required level if a sufficient type and/or number of links and/or nodes in the network are disabled or destroyed.[83] In order to act with the maximum initiative and render an enemy system/network inoperative with more certainty, target system intelligence is required to

---

[81] Slessor, *Air Power and Armies*, 136. Wreckage can be cleared and damage repaired. "Immediately on receipt of the report of a successful attack on a railway, arrangements should be made for the constant harassing of the crash by relays of aircraft at the shortest possible intervals[.]"

[82] Slessor, *Air Power and Armies*, 122. Air power "depends for its effect far more upon dislocation and disorganization than upon actual material damage."

[83] Barabási, *Linked : The New Science of Networks*, 113-19. For any network, there exists a critical number, for which if that number of nodes are randomly removed from a network, the network will abruptly fail. In scale free networks, which are characterized by hubs that have a disproportionate number of links compared to other nodes in the network, disabling a few hubs will cause the network to rapidly collapse.

orient air attacks properly, precisely because the effects of air power are necessarily indirect.

The nature of cyber power is systemic or networked. Because indirect effect is a feature of any attack on a network, and cyberspace is inherently networked, using cyber power with maximum initiative also requires target system intelligence. If attacks are not satisfactorily oriented, they will not create effects that contribute to achieving military objectives, making the initiative advantage inherent in cyber power's speed worthless. Therefore, effective and efficient employment of cyber power requires sufficiently accurate and precise system intelligence on both network architecture and function. As system complexity increases, the intelligence burden grows. Consequently, air power devotes significant effort to intelligence preparation of the battlespace. Cyber power must do the same. Cyber power too must be properly oriented to maximize desirable, and minimize undesirable, effects precisely because cyber power effects are inherently indirect.

Thus intelligence is critical for air and cyber attack, but it is also critical for air and cyber defense. The invention of radar restored a speed ratio of intelligence to preparation that reduced an air attacker's advantage of initiative to a level allowing for practical, general air defense. Radar, for a time, permitted the defense to concentrate forces and engage the air attacker at a time and place that allowed the defense to achieve its object of preservation. This state of affairs was brief because it led to a back and forth game played in the electromagnetic spectrum known today as electronic warfare. The advantage of air attack over air defense in large measure depends on who holds the advantage in electronic warfare.

Electronic warfare within air warfare can be thought of as a contest to alter the speed ratio of intelligence to preparation to one's advantage. Like cyber warfare, electronic warfare occurs at the speed of light. Consequently, electronic warfare inheres a speed ratio of intelligence to preparation that favors electronic attack over electronic defense. A limit of known physics is that faster than speed of light transport for anything, including data, is a practical impossibility for the forseeable future. Thus this speed ratio will likely persist well into the future, favoring electronic and cyber attack over defense

for a long time to come. The logical conclusion is that effective electronic and cyber defense are impossible. However, in reality, electronic attack has not been favored over electronic defense continuously. The electronic defender cannot overcome the speed ratio problem, except if he already knows the character of the attack such that the speed of preparation is virtually nil.

As Corbett described, effective defense requires the speed of intelligence to be much, much greater than the speed of preparation. Until the advent of electronic warfare, combatants typically sought ways to increase the speed of intelligence by seeking the high ground as well as by developing faster modes of transportation and communication. This method is unavailable to electronic warfare practitioners. However, a similar result for the defense is possible by reducing the speed of preparation to zero. Any number divided by zero yields a mathematically infinite result. Thus a speed ratio of intelligence to preparation, in which the speed of preparation is zero or very close to it, is very large, changing the dynamics of combat to facilitate a practicable defense. In electronic warfare, the speed of preparation is reduced to zero through intelligence that enables defensive preparation well in advance of combat. Because a speed ratio based on speed of light action is inherent to cyber power like electronic warfare, practicable cyber defense is only possible through intelligence well in advance such that the speed of preparation falls to zero. Since the magnitude of the initiative advantage for air power depends on an electronic warfare initiative advantage that depends on intelligence, who holds the initiative advantage depends on the relative quality of intelligence between combatants. Superior intelligence in air and cyber power allows one’s nearly instantaneous actions, crucially, to be satisfactorily oriented. The initiative advantage in air and cyber power rests largely on preparation, supported by good intelligence, well before conflict begins. Intelligence drives air power and cyber power operations.

CHAPTER 3

THE ESTONIA AND GEORGIA CYBER CONFLICTS

Two of the most notable and studied incidences of cyber warfare are the 2007 conflict in Estonia and the 2008 conflict in Georgia. Although cyberspace's importance had been growing for more than 50 years, these two conflicts, closely spaced, drove home how much the domain had become interwoven into the fabric of modern society. These two conflicts focused mass attention on cyber power and its utility in war in a way that previous cyber power uses had not. The high profile of these two conflicts caused them to become the subject of much study. Resultantly, these two conflicts are a rich source of information on the dynamics of cyber attack and defense. The following details of these two conflicts provide the raw material for comparisons of cyber power to land, sea, and air power. The comparisons will demonstrate that the analogies of cyber power to land, sea, and air power made up to this point are supported by experience in the real world. Additionally, raw material from other occurrences of cyber warfare, like the Stuxnet cyber attack, will be interwoven into the analysis. However, these occasions represent a minor source for analysis so their relevant details are not included in this chapter, but will be given as the need arises.

2007 – Cyber Combat in Estonia

Geographically, Estonia borders Latvia to the south, Russia to the East, the Baltic Sea to the west, and the Gulf of Finland to the north.[1] As the crow flies, Estonia is about 100 miles from St. Petersburg and even closer to the Finnish capital of Helsinki across the gulf to the north. Demographically, Estonia is 24.9 percent ethnic Russian.[2]

---

[1] "Estonia Map," *National Geographic*, http://travel.nationalgeographic.com/travel/countries/estonia-map/ (accessed 23 March 2011).

[2] Department of State, "Background Note: Estonia," http://www.state.gov/r/pa/ei/bgn/5377.htm (accessed 24 March 2011).

Historically, Estonia has been part of Russia's sphere of influence. Estonia was part of the Russian Empire until the end of World War I.[3] Estonia enjoyed a brief period of independence during the Interwar Years until it was incorporated into the Soviet Union in 1940 as part of Joseph Stalin's 1939 peace pact with Adolph Hitler.[4] After Nazi Germany broke the peace pact and attacked the Soviet Union, the Nazis occupied Estonia from 1941 until the Red Army liberated the country in 1944.[5] Estonia declared its independence from the Soviet Union in 1991 during the Soviet coup, but did not gain its full independence until 1994, when Russian Federation armed forces withdrew from Estonia.[6] Since then, Estonia has turned its gaze West. Estonia became a member of both NATO and the European Union in 2004.[7]

Estonia's shift in focus to Europe coincided with a significant investment in cyberspace. By 2007, 97 percent of all Estonia's bank transactions occurred online, and 60 percent of the population used the Internet daily.[8] The government had fully integrated the Internet into its operations, including voting. For instance, 5.5 percent of votes in the February 2007 elections were cast via the Internet, and 86 percent of Estonians did their taxes online in 2006.[9] By April 2007, Estonia had become heavily dependent on cyberspace for the nation's daily functioning, or so it seemed.

Strong Russian influence throughout Estonia's history, a significant ethnic Russian minority, and perceived cyber dependence were significant factors in precipitating the 2007 cyber attacks on Estonia. However, the government decision, symbolic of diminished Russian sway over Estonia, was the proverbial straw that broke the camel's back. On 26 April 2007, Estonia moved a statue commemorating the Red

---

[3] Department of State, "Background Note: Estonia."

[4] Department of State, "Background Note: Estonia." "Leading up to World War II, Estonia pursued a policy of neutrality. However, the Soviet Union forcibly incorporated Estonia as a result of the Molotov-Ribbentrop Pact of 1939, in which Nazi Germany gave control of Estonia, Latvia, and Lithuania to the Soviet Union in return for control of much of Poland. In August 1940, the U.S.S.R. proclaimed Estonia a part of the Soviet Union as the Estonian Soviet Socialist Republic."

[5] Department of State, "Background Note: Estonia."

[6] Department of State, "Background Note: Estonia."

[7] Department of State, "Background Note: Estonia."

[8] Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs*, no. Winter/Spring (2008), http://www.europeaninstitute.org/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html (accessed 24 November 2010).

[9] Merike Kaeo, *Cyber Attacks on Estonia: Short Synopsis*, 2 May 2007, http://www.doubleshotsecurity.com/pdf/NANOG-eesti.pdf (accessed 27 Nov 2010).

Army's heroism in liberating the Estonian capital of Tallin from the city's center to a military cemetery in the suburbs.[10] The movement of the statue triggered a cyber attack on Estonia by ethnic Russians within and outside the country.[11] The statue's movement caused ethnic Russians in Tallin to riot, but the cyber attacks that followed are what caught the world's attention.[12] The start of the cyber attacks coincided with the riots in Tallin.[13] Although, the physical riots were quelled relatively quickly, the cyber assault continued for weeks.[14]

The cyber attacks did not come as a strategic surprise to Estonia. Prior to the conflict, Estonia was aware that a large-scale cyber attack was being planned against it based on discussions held in Russian-language Internet forums.[15] The cyber attack was fueled by simple, step-by-step instructions and a pre-selected target list posted within these forums.[16] The cyber assaults primarily consisted of what is known in cyber circles as distributed denial of service (DDoS) attacks.[17] DDoS attacks target the flow of information within a cyber network by bombarding the servers, routers, and switches that direct traffic on the network with swarms of data.[18] The object of a DDoS attack is to create a cyber traffic jam so that information cannot flow efficiently through the network, denying users the use of the network to perform their tasks. In this case, the attackers generated the volume of traffic necessary to clog Estonia's computer networks by organizing an ad hoc cyber militia through the Russian-language Internet forums and by employing botnets.[19] A botnet is a third-party, centrally controlled and directed network

---

[10] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 August 2007, http://wired.com/politics/security/magazine/15-09/ff_estonia (accessed 3 January 2011).

[11] Davis, "Hackers Take Down the Most Wired Country in Europe."

[12] Davis, "Hackers Take Down the Most Wired Country in Europe."

[13] Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs* 9, no. 1 (2008): 123-24.

[14] Mark Landler and John Markoff, "In Estonia, what may be the first war in cyberspace," *New York Times*, 28 May 2007, http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html?pagewanted=1&_r=1 (accessed 24 March 2011).

[15] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 122.

[16] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.

[17] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[18] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[19] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.

of hundreds of thousands of computers, previously hijacked by hackers with Trojan-horse software that turns unsuspecting owners' computers into *zombies*.[20]

The cyber attack was massive. More than one million computers globally were hijacked and turned into zombies for the assault.[21] The cyber attack's magnitude varied during the course of the conflict, but the ten largest waves blasted streams of data into the Estonian network at 90 megabits per second, lasting up to 10 hours each.[22] The cyber aggressors also attempted to maximize their efforts beyond the blind use of simple mass. For example, at least one botnet attack used specially constructed code to exploit specific Estonian cyber vulnerabilities.[23] In one instance, the attackers sent a single, huge data burst to measure network capacity.[24] Hours later, data from multiple sources flowed into the network rapidly saturating the capacity of its routers and switches.[25]

The assault on Estonian cyberspace lasted for several days before it finally climaxed in a crescendo of activity starting 9 May 2007, the May Day holiday celebrating Russia's victory over Nazi Germany.[26] During the early hours of 9 May 2007, Estonian Internet traffic spiked to a level 1,000 times greater than normal, with even heavier traffic on 10 May.[27] None of the subsequent cyber barrages ever equaled the magnitude of the 9-10 May onslaught. The cyber conflict effectively ended with the last major wave of attacks on 18 May.[28]

Estonia's initial defense was simple – it temporarily shut down access to Estonian websites from abroad.[29] "This defense – the modern equivalent of pulling up the drawbridge to protect a medieval castle – was a temporary stratagem that allowed time

---

[20] Davis, "Hackers Take Down the Most Wired Country in Europe." Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.

[21] Ruus, "Cyber War I: Estonia Attacked from Russia."

[22] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[23] Gadi Evron and Hillar Aarleid, "Estonia: Information Warfare and Lessons Learned," in *Workshop on Learning from Large Scale Attacks on the Internet - Policy Implications* (Brussels, Belgium: European Commission, 2008), 18.

[24] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[25] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[26] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[27] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[28] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[29] Ruus, "Cyber War I: Estonia Attacked from Russia." Davis, "Hackers Take Down the Most Wired Country in Europe."

for counterattack as the ultimate defense."[30] Estonia had this option because it possessed high capacity external Internet links through Finland, Sweden, Latvia, and Russia, owned by multiple network operators, across which data could be dispersed, as well as sufficient internal Internet connectivity to allow Estonia to sever external Internet connections with acceptable, short-term cyber degradation.[31] Beyond this temporary fix, Estonia used a three-pronged cyber defense strategy.[32] First, Estonia sought to quickly bolster its server capacity.[33] Second, the nation tried to filter out the zombie attack traffic from reaching the country's servers.[34] Lastly, Estonia located the enemy botnets and zombies to neutralize them, in other words, it counterattacked.[35]

Four days after Estonia took refuge behind its virtual castle walls and cut off most international Internet connectivity, Hillar Aarelaid, director of Estonia's Computer Emergency Response Team (CERT), was fortunate enough to have dinner with Kurtis Lindqvist. Lindqvist ran one of the world's 13 root domain name servers, and was a member of the Vetted.[36] The Vetted are a few individuals trusted by the world's largest Root Internet Service Providers (ISPs) to remove rogue computers from the network.[37] Lindqvist and two other members of the Vetted attending a meeting in Tallin agreed to help Aarelaid.[38] This started the third prong of Estonia's cyber defense, the counterattack.

On the night of 8 May, Aarelaid and the three members of the Vetted went to the Estonian CERT headquarters in anticipation of the May Day cyber onslaught.[39] At exactly midnight Moscow time on 9 May, the attack started to squeeze all of Estonia's Internet capacity.[40] The CERT set-up online chat rooms to provide a safe forum where

---

30 Ruus, "Cyber War I: Estonia Attacked from Russia."

31 Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallin, Estonia: Cooperative Cyber Defense Centre of Excellence, 2008), 6.

32 Ruus, "Cyber War I: Estonia Attacked from Russia."

33 Ruus, "Cyber War I: Estonia Attacked from Russia."

34 Ruus, "Cyber War I: Estonia Attacked from Russia."

35 Ruus, "Cyber War I: Estonia Attacked from Russia."

36 Davis, "Hackers Take Down the Most Wired Country in Europe."

37 Davis, "Hackers Take Down the Most Wired Country in Europe."

38 Davis, "Hackers Take Down the Most Wired Country in Europe." Ruus, "Cyber War I: Estonia Attacked from Russia."

39 Davis, "Hackers Take Down the Most Wired Country in Europe."

40 Davis, "Hackers Take Down the Most Wired Country in Europe."

Estonia's cyber defenders from across the region and all relevant organizations could communicate real-time information on attack targets and types.[41] Aarelaid's team immediately started tracing the Internet Protocol (IP) addresses as the Vetted sent e-mails to the ISPs to block the attacking zombies and hacktivists.[42] The attack was thwarted, and by dawn Estonia's Internet traffic hovered just above normal.[43]

The cyber attackers did not sit idly while the Estonian CERT executed their defense. Fresh posts continuously updated the blogosphere with new targets and attack instructions.[44] When the cyber attacks from abroad were beaten back, botnet assaults were launched from zombies hijacked inside Estonia.[45] Even in cyberspace, warfare is a dynamic interaction between adaptive adversaries.

In the final analysis, the cyber attack was well organized and planned.[46] Despite enemy planning, the cyber attack caused only modest, temporary, and surprisingly little damage.[47] Customers of the country's two largest banks could not access their accounts for a few hours.[48] Some of Estonia's primary news outlets had their Internet portals disrupted and temporarily had to shut down international access.[49] Lastly, although 97 percent of all bank transactions occur online in Estonia and 60 percent of the population uses the Internet daily, the cyber attack from April to May 2007 did not affect most of the nation's ordinary citizens.[50]

2008 – Cyber Combat in Georgia

In demographic terms, 83.8 percent of Georgia's population is mostly ethnic Georgian with the remainder consisting of Azeri, Armenian, Russian, and other ethnic

---

[41] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 124.

[42] Davis, "Hackers Take Down the Most Wired Country in Europe."

[43] Davis, "Hackers Take Down the Most Wired Country in Europe."

[44] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123.

[45] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.

[46] Evron and Aarleid, "Estonia: Information Warfare and Lessons Learned," 18.

[47] Ruus, "Cyber War I: Estonia Attacked from Russia."

[48] Ruus, "Cyber War I: Estonia Attacked from Russia." Landler and Markoff, "In Estonia, what may be the first war in cyberspace."

[49] Ruus, "Cyber War I: Estonia Attacked from Russia."

[50] Ruus, "Cyber War I: Estonia Attacked from Russia."

groups.[51] Geographically, Georgia shares its northern border with Russia.[52] To the west is the Black Sea, to the east is Azerbaijan, and to the south lays Turkey, Azerbaijan and Armenia. With respect to geography, Estonia and Georgia are similar in that both share a large border with Russia and each have access to the sea.

Though not very ethnically diverse, Georgia's roots run deep with more than 2,500 years of recorded history.[53] For most of the 19th and 20th centuries, Georgia was ruled by Russia.[54] Like Estonia, Georgia enjoyed a brief period of independence during the Interwar Years after WWI.[55] On 9 April 1991, Georgia declared its independence from the Soviet Union.[56] Since then, Georgia like Estonia has looked more to the West than toward Russia. Georgia is seeking membership in NATO and the EU, though it did not enjoy the protection of either group in 2008.[57]

Following Georgian independence, secessionists seized control of the majority of Abkhazia and portions of South Ossetia before cease-fire agreements were reached in 1992 and 1994.[58] These conflicts remain unresolved, and led to the five-day war between Russia and Georgia in 2008.[59] Similar to the Estonian incident the previous year, cyber power's role in the 2008 Russia-Georgia war drew significant world attention.

Despite other geo-strategic similarities, Georgia and Estonia differed significantly in the cyberspace domain. Just 7 percent of Georgia's citizens used the Internet daily compared to 60 percent of Estonians.[60] More than half of Georgia's 13 connections to the worldwide Internet passed through Russia.[61] Most of Georgia's 309 Internet prefixes were routed through Turkish or Azerbaijani ISPs, though the latter were then routed

---

[51] Department of State, "Background Note: Georgia," http://www.state.gov/r/pa/ei/bgn/5253.htm (accessed 26 March 2011).
[52] Department of State, "Background Note: Georgia."
[53] Department of State, "Background Note: Georgia."
[54] Department of State, "Background Note: Georgia."
[55] Department of State, "Background Note: Georgia."
[56] Department of State, "Background Note: Georgia."
[57] North Atlantic Treaty Organization, "NATO's relations with Georgia," http://www.nato.int/cps/en/natolive/topics_38988.htm (accessed 29 May 2011).
[58] Department of State, "Background Note: Georgia."
[59] Department of State, "Background Note: Georgia."
[60] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 5. Ruus, "Cyber War I: Estonia Attacked from Russia."
[61] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 6.

through Russia.[62] In other words, Georgia's Internet infrastructure suffered from a dearth of internal connections known as Internet exchange points.[63] Consequently, a Georgian web surfer's request for a Georgian web page would likely be routed outside the country, like having to travel through Mexico in order to get from Los Angeles to San Francisco.[64] With a large percentage of Georgia's Internet connectivity, internal and external, under direct Russian influence, Georgia had few cyber defense options in a conflict with Russia.[65] Lacking multiple external Internet exchange points and internal connectivity in its Internet architecture, Georgia could neither disperse network traffic, nor cut Internet connectivity from abroad like Estonia without rendering Georgian cyberspace essentially useless.[66]

The Georgian cyber conflict differed from the Estonian one in another crucial aspect – the cyber conflict in Georgia coincided not with mere riots, but an actual shooting war between the organized military forces of two nations. The 2008 Georgia-Russia war officially started on 7 August after Georgian military forces responded to alleged Russian provocation with a massive artillery barrage on the town of Tshkinvali in South Ossetia .[67] Russia seized the opportunity to further solidify South Ossetia's and Abkhazia's independence from Georgia. Russia immediately deployed more troops to South Ossetia and initiated bombing raids on Georgian territory.[68] Russia also deployed its navy in order to blockade the Georgian coast, as well as landed marines on the coast of Abkhazia.[69] Russian mechanized forces and South Ossetian militia defeated the lightly armed Georgian military around Tskhinvali and then invaded Georgian territory uncontested.[70]

---

[62] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 6.

[63] Ben Arnoldy, "Cyberspace: new frontier in conflicts," *The Christian Science Monitor*, 13 August 2008, http://www.csmonitor.com/USA/Military/2008/0813/p01s05-usmi.html (accessed 17 January 2011).

[64] Arnoldy, "Cyberspace: new frontier in conflicts."

[65] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 6.

[66] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 6.

[67] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal.com*, 6 January 2011, 1, http://www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (accessed 13 January 2011).

[68] Hollis, "Cyberwar Case Study: Georgia 2008," 1.

[69] Hollis, "Cyberwar Case Study: Georgia 2008," 1.

[70] Hollis, "Cyberwar Case Study: Georgia 2008," 1.

The Russian war against Georgia in 2008 appeared to be a joint military campaign that harnessed land, sea, air, and cyber power. While the cyber attack could not be attributed to the Russian government, cyber operations were synchronized with military operations in the other warfighting domains.[71] Had the cyber attack on Georgia been less integrated with military operations in the physical domains, the cyber assault would probably not have exhibited the precision in scope and concentration of effort that characterized cyber warfare in this conflict. To illustrate, the total number of botnet cyber targets never exceeded 11, and the same websites continued to be attacked throughout the war.[72]

The cyber attack against Georgia was two-pronged in that it included both website defacements and DDoS attacks.[73] Botnets prepared in advance executed the first cyber attack wave.[74] After this wave, the assaulting cyber effort expanded when cyber attack tools and a list of suggested targets were posted on websites for ad hoc cyber militia members to wield.[75] The postings amateurized cyber warfare; the cyber attack instructions were simple enough for people with limited computer skills to apply effectively.[76] This cyber militia was so effective that it shut down or defaced 43 websites beyond the original 11 botnet targets.[77] 54 Georgian websites related to communications, finance, and government were struck such that Georgians could not access the sites for information or instructions.[78]

---

[71] John Bumgarner and Scott Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008* (U.S. Cyber Consequences Unit, 2009), 2-3. The timing with respect to military operations suggests close coordination between the cyber attack and conventional Russian military operations.

[72] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[73] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[74] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[75] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[76] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[77] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[78] John Oltsik, "Russian Cyber Attack on Georgia: Lessons Learned?," *Network World*, http://www.networkworld.com/community/node/44448 (accessed 27 March 2011). Bumgarner and Borg,

While the cyber attacks were simple technically, they were operationally sophisticated.[79] Most of the cyber attack tools were customized for Georgian targets, with at least one website defacement prepared more than two years prior to the conflict.[80] The cyber attacks were also sophisticated in their targeting. Government and news media websites were targeted first so that Georgian officials would have difficulty determining what was actually happening, as well as to delay any international response.[81] In addition to Georgia's two big banks, the attack targeted commercial entities that could have been used to communicate and to help coordinate a response to the attack.[82] At first glance it seems odd, but educational institutions devoted to science, technology, and medicine were also attacked in the cyber assault.[83] However, when one considers that a popular Georgian hacker forum was also among the early DDoS targets, the rationale for cyber attacks on educational institutions becomes clear.[84] Hacker forums are sources of cyber expertise that Georgia could have used to parry the cyber attack. Additionally, CERT Georgia, the organization that eventually assumed the role of national CERT, normally provided cyber security technical support for Georgia's higher education institutions as part of the Georgian Research and Educational Networking Association (GRENA).[85] By attacking educational institutions, the cyber attackers probably occupied CERT Georgia with its charter mission to protect GRENA's cyberspace, and delayed the nation from enlisting the CERT to address the larger national cyber crisis sooner. When the adversary attacked Georgian hacker forums and their educational institutions, the enemy

---

Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008, 4. Hollis, "Cyberwar Case Study: Georgia 2008," 2.

79 Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

80 Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4-5.

81 Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 5.

82 Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 5.

83 Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 5.

84 Greg Keizer, "Russian hacker 'militia' mobilizes to attack Georgia" *Network World.com*, 13 August 2008, http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html (accessed 17 January 2011). Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 12.

85 Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14-15. Georgian Research and Educational Networking Association (GRENA), http://www.grena.ge/eng/cert.html (accessed 27 March 2011).

neutralized Georgia's latent cyber defense forces. Lastly, specific geographic locales were targeted just prior to the commencement of traditional combat operations in that region.[86] For example, in the town of Gori, government and news websites were disabled with DDoS attacks just prior to a Russian air attack.[87]

The cyber attack on Georgia was operationally sophisticated, unfortunately Georgia's cyber defense was not. Some Georgian websites simply remained online without change, taking no additional defensive steps.[88] Some, like the websites of the President, the Ministry of Defense, and the Ministry of Foreign Affairs, were moved to servers outside the country.[89] Georgia also attempted to filter out the cyber attacks based on their originating IP address, but the attackers easily circumvented these filters by using foreign servers to mask their real IP addresses or using software to create a false IP address.[90] Lastly, Georgia attempted at least one major counterattack. Georgia posted cyber attack tools and instructions in Russian-language Internet forums to deceive the hostile cyber militia members into unknowingly attacking Russian websites instead of Georgian ones.[91] The effect of the Georgian cyber counterattack on Russian websites appears to have been negligible.[92] While Georgia's cyber defense preserved the use of some government websites, overall it was too little too late.

The cyber attack appeared to achieve its primary military objective of disrupting communications in Georgia. In particular, the volume of cyber attack traffic effectively jammed traditional communications, seriously disrupting e-mail, landline phone calls, and cell phone calls during parts of the campaign.[93] Georgia felt this effect most acutely

---

[86] Hollis, "Cyberwar Case Study: Georgia 2008," 5.

[87] Joseph Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government," *Los Angeles Times*, 13 August 2008, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html (accessed 27 March 2011)..

[88] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14.

[89] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (2008): 66-67. Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14.

[90] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 7.

[91] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 7.

[92] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 7.

[93] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 6.

in the early stages of the war, when efficient communication was most critical in organizing a coordinated response.[94] The operational effects of the cyber attacks on Georgia and Estonia were temporary, but their impact on the development of cyber power continues to ripple throughout the world.

[94] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 16.

CHAPTER 4

TERRAIN AND FORTRESSES IN LAND AND CYBER POWER

Terrain and fortresses are two determinants of strategic advantage in land power and cyber power.[1] The complexity of cyberspace, particularly the syntactic layer (software), is similar to mountainous terrain. This complexity means that vulnerabilities are inherent within cyberspace and that an adversary with enough time and resources will eventually find an unguarded or lightly guarded approach through which to breach the defense, just as in mountain warfare. Cyberspace's speed and automation allow cyber power to generate mass akin to the *levee en masse* during the Napoleonic period. For land power, the *levee en masse* changed the utility of fortresses in defense.

Fortresses morphed from a primary means to protect what was inside the fortress walls, to a means mainly used to weaken an attack on a theater of operations.[2] The *levee en masse* allowed armies to be formed with sufficient size that one could lay siege to multiple fortresses and continue to attack deeper into the theater with maneuver forces. A similar situation exists with cyber power. Cyber power can lay siege to multiple enclaves' firewalls while continuing to press a cyber attack in other regions of cyberspace. Since the *levee en masse*, fortresses have functioned to force an opponent to invest them. In this way, fortresses decreased the number of maneuver forces able to continue an attack deeper into a theater of operations, slowing and weakening the assault, thus buying time for defense reinforcements to arrive. Ultimately, fortresses serve to help bring an attacker to culmination, changing the ultimate balance of strength in favor of the defender in land and cyber warfare, not to simply preserve what is within the fortress walls.[3]

---

[1] Clausewitz, *On War*, 363.

[2] Clausewitz, *On War*, 394, 497.

[3] Clausewitz, *On War*, 566-73. An attacker has been brought to culmination when he has reached the point beyond which effective self-defense for the attacker is impossible. A good system of fortresses

The Battle of Monte-Cassino in World War II (WWII) illustrates that Clausewitz's conclusions about mountain warfare operate in the real world. The French experience at Na San and Dien Bien Phu in Indochina are exemplars of how the use of fortresses can fail in war when not used in accordance with the concepts Clausewitz proscribed. However, US defense of the Pusan perimeter in the Korean War demonstrates how a fortress can be used successfully to change the balance of strength in favor of the defender. Elements of the cyber conflicts in Estonia and Georgia parallel each of these examples from land warfare.

Levee en Masse

There is no need to recount the details of the French *levee en masse* under Napoleon. Suffice it to say, French people rose up in revolution and put armies into the field the size of which were unprecedented to that point in history. These new armies changed the value of fortresses in warfare from ultimately protective structures to weakening and delaying devices. The *levee en masse* was made possible by the amateurization of warfare, facilitated by the invention of the musket and drill training to instill discipline.[4] These innovations allowed states to put armies into the field with a level of training that would have been suicidal before then. Speed of action and automation in cyber power create a similar dynamic that has led to the amateurization of cyber warfare.

The Estonian and Georgian cyber conflicts of 2007 and 2008 exposed the amateurization of cyber warfare. In both conflicts, botnets – centrally controlled large networks of computers – were used to launch distributed denial of service (DDoS) attacks on multiple websites and Internet servers simultaneously. In this way, a few individuals controlled a large, disciplined cyber army of computers, numbering almost one million in size against Estonia in 2007.[5] Cyber attackers rapidly and substantially increased their force's size by using the *mass medium* of cyberspace to self-publish attack software,

---

helps the defender cause the attacker to reach culmination sooner rather than later, thus mitigating damage and increasing what the defense can preserve.

[4] J. F. Guilmartin quoted in Parker, *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800*, 17. "Where a few days and a good drill sergeant might suffice to train a reasonably good [musketeer], many years and a whole way of life were needed to produce a competent archer."

[5] Ruus, "Cyber War I: Estonia Attacked from Russia."

simple instructions, and a list of targets in Russian-language hacker forums.[6] In the Georgian conflict, an amateur cyber militia, also called script kiddies, was able to carry the cyber attack well beyond the 11 targets that botnets initially assaulted.[7] The cyber militia increased the number of servers and websites under seige four fold.[8] The very moniker given to these cyber militiamen indicates the level of amateurization possible in cyber warfare – script *kiddies*. A cyber militia led and equipped by an able cyber warrior needs skills so simple that the *a priori* proficiency of *children* is sufficient to mount an effective cyber attack. Even Napoleon's *levee en masse* required young men. The scope of the possible in a cyber *levee en masse* is so complete that virtually everyone, including children, with a computing device connected to the Internet, as well as all idle devices connected to the Internet, is a latent cyber combatant. Automation makes it simple for an amateur to be an effective cyber soldier, because automation masks cyberspace's complex, mountainous character from these novices.

Cyberspace Is Mountainous

Like the complexity of mountainous terrain, the complexity of software that makes up the syntactic layer of cyberspace gives it a mountainous character. In mountainous terrain on land or in cyberspace, an attacker will eventually find a vulnerable opening through which to gain access to friendly territory, given enough time and resources. The Germans and Allies observed this lesson in land warfare at the Battle of Monte-Cassino in WWII.

The Battle of Monte-Cassino

Monte-Cassino is a town in the Liri Valley along Route 6, a road in Italy running north from Naples to Rome.[9] The Monte-Cassino Monastery towers over the valley entrance, built on more than 500 meters of solid rock that rises almost vertically from the

[6] Davis, "Hackers Take Down the Most Wired Country in Europe." Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[7] Davis, "Hackers Take Down the Most Wired Country in Europe." Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[8] Davis, "Hackers Take Down the Most Wired Country in Europe." Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4.

[9] Matthew Parker, *Monte Cassino: The Hardest-Fought Battle of World War II* (New York, NY: Doubleday, 2004), xiii.

valley floor.[10] From the valley to the coast lie the Aurienci Mountains, and behind Cassino Massif rises the Abruzzi Mountain Range.[11] This set of mountains was the last natural defensive position for the Germans between the Allies and Rome as they advanced north from Naples.[12] Along this extent of mountains, the Germans formed the Gustav Line to make a defensive stand. The line was anchored by the German position on Cassino Massif, which commanded all approaches to the Liri Valley, the only viable path to Rome for Allied armor.[13]

The German defensive works were formidable. The Gustav Line consisted of a series of interlocking defenses.[14] The line was multi-layered, with prepared fall-back positions from which to launch counterattacks on front areas lost.[15] However, these strong points did not provide mobile reinforcements to each other during engagements by way of flanking counterattacks on the Allies, because the terrain prohibited it from occurring with the required speed.[16] The Germans had time to survey every possible route of attack and take countermeasures.[17] Despite these countermeasures, the Germans were unable to hold the Gustav Line.

The battle started on 15 January 1943, and did not come to a close until 18 May 1943, when the defeated German force hoisted a white flag over the destroyed Monte-Cassino Monastery.[18] It took the Allies four big attempts to take Cassino. During the fourth attempt, a French general, General Juin, leading the French Expeditionar y Corps (FEC), finally broke through the Gustav Line.[19]

---

[10] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, xiii-xiv.

[11] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, xiv.

[12] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, xv.

[13] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, xiii-xiv.

[14] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, xv.

[15] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, xv.

[16] Dominick Graham and Shelford Bidwell, *Tug of War: The battle for Italy, 1943-1945* (New York, NY: St Martin's Press, 1986), 303-07. For example, once the Allies pierced the Gustav Line in General Juin’s sector and cut the Ausonia-Ausente lateral road, the Allies would have the terrain advantage and the German defenders would find it difficult if not impossible to move reserves into the area given the rough, mountainous terrain. Boxed in, the nature of the terrain was a hindrance as much as a help to the German defenders.

[17] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, xv.

[18] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, 77,332.

[19] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, 272. The Germans were most concerned with where and when General Juin’s French Expeditionary Corps would attack.

During the Allies' victorious fourth attempt to take Cassino and break the Gustav Line, the Allies enjoyed a three to one advantage in troops.[20] However, Allied troop mass was not the primary factor that enabled the FEC to break through the line. The FEC broke through the Gustav Line where the German defense was weak, not because of overwhelming mass at the point of attack.

The FEC was positioned in front of the Aurienci Mountains running from the Liri Valley to the coast.[21] The Germans considered this terrain too tough for a major Allied assault, so the approaches were very lightly defended.[22] Mountainous terrain is complex, and has a myriad number of paths through it if one is willing to exert the effort.[23] It is impossible to defend all of these paths given the reality that resources are finite. General Juin and his FEC exploited this fact, but only after the Allies spent five months of fighting and shed rivers of blood before they stumbled on the weakness in the German defense.[24] Unfortunately for the Germans, their Prussian predecessor proved correct in his observations about defense in mountainous terrain. Clausewitz' observations about warfare in mountainous terrain apply to cyberspace as well.

Complexity in Estonian and Georgian Cyberspace

In Estonia and Georgia, cyber attackers exploited what in hindsight were clear vulnerabilities. If the terrain of cyberspace resembles mountains, then it should be complex and require a significant investment of time and effort to find exploitable cyber vulnerabilities. How is it that the Allied victory at Monte-Cassino took months of fighting to find a soft spot in the Gustav Line, but the cyber attackers in Estonia and Georgia exploited cyber vulnerabilities on day one of their attacks without having to probe for weaknesses? The answer is intelligence.

---

[20] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, 274.

[21] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, 278.

[22] Parker, *Monte Cassino: The Hardest-Fought Battle of World War II*, 278.

[23] Clausewitz, *On War*, 420. Mountainous terrain may be impassable to large columns, but that does not equate to being inaccessible to infantry.

[24] Graham and Bidwell, *Tug of War: The battle for Italy, 1943-1945*, 313-14. For example, the Allied forces break the position at Castelforte not with a massive frontal assault, but with infiltration tactics. As Clausewitz described, mountainous terrain may be impassable but that does not mean inaccessible as the Allies demonstrated at Castelforte.

There are two ways to find a path through complex, mountainous terrain. The first is to employ the method of trial and error *after* the commencement of hostilities as the Allies did at the Battle of Monte-Cassino. The Allies did so out of necessity. Had they a choice, the Allies certainly would have chosen the second way – to gather intelligence on the terrain and defenses to identify weak points *before* hostilities started. The cyber attackers against Estonia and Georgia used the second approach.

The cyber attackers against Estonia and Georgia did not have to exert significant effort to find exploitable cyber vulnerabilities during the conflict because they had already done so before the conflict started. The evidence for this is circumstantial. For example, when the cyber attacks began against Georgia, the attack jumped straight to the type of assault best suited to the particular target under attack without a reconnaissance phase.[25] In Estonia, at least one botnet attack used specially made computer code that specifically targeted Estonian cyber vulnerabilities.[26] The absence of cyber probing by the attackers in the Georgian conflict implies that such probing was done in advance.[27] Prior to these attacks, one can reasonably infer that the exploited cyber vulnerabilities were far less apparent, else a state as integrated into cyberspace as Estonia would have taken greater measures in advance to avoid the cyber crisis they faced in 2007. The argument that cyberspace is mountainous, thus requiring intelligence to mount an effective attack, is further supported by the fact that one Georgian website defacement was prepared at least two years in advance.[28] In the case of Estonia, the presence of zombie computers inside the country, functioning as part of a botnet attack force, suggests significant prior preparation by the cyber attackers to penetrate the individual defenses of these computers and hijack them with Trojan-horse software.[29] These examples support, although indirectly, the observation that cyberspace is analogous to

---

[25] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 3.

[26] Evron and Aarleid, "Estonia: Information Warfare and Lessons Learned," 18.

[27] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 3.

[28] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 5.

[29] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.

complex, mountainous terrain, necessitating time-consuming reconnaissance to identify lightly defended approaches.

The recent Stuxnet cyber attack on Iran's nuclear program provides better evidence of the complex, mountainous character of cyber terrain. Stuxnet is a computer worm that disabled one fifth of Iran's nuclear centrifuges, essential components in the uranium enrichment process to produce nuclear weapons.[30] In order to verify Stuxnet would work, the virus had to be tested. Consequently, the work to find and exploit cyber vulnerabilities in Iran's nuclear centrifuges started years in advance.

After a test at Idaho National Laboratory, cyber vulnerabilities to the Siemens supervisory control and data acquisition (SCADA) system controlling the Iranian nuclear centrifuges were made public at the 2008 Automation Summit in Chicago, Illinois.[31] The details of these vulnerabilities were not made public, but these vulnerabilities were exploitable by any who could gain access to the Siemens test data, legally or otherwise.[32] Recent analysis of Stuxnet's code by a private computer security firm, after the cyber attack became public in 2010, concluded that the virus could only have been created by someone who knew the specific quirks of Siemens' SCADA, and had intimate understanding of Iran's uranium enrichment centrifuge operations.[33] Gaining this intimate intelligence appears to have started years in advance, at least as early as 2003, if not as early as the 1980s.[34]

The Stuxnet cyber attack required years of intelligence exertion. Stuxnet required *intimate* and *nuanced* knowledge of the paths traveling through the cyber terrain of Iran's

[30] Broad, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay."
[31] Broad, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay."
[32] Broad, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay."
[33] Broad, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay."
[34] Broad, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay." "The account starts in the Netherlands. In the 1970s, the Dutch designed a tall, thin machine for enriching uranium. As is well known, A. Q. Khan, a Pakistani metallurgist working for the Dutch, stole the design and in 1976 fled to Pakistan…The resulting machine, known as the P-1, for Pakistan's first-generation centrifuge, helped the country get the bomb. And when Dr. Khan later founded an atomic black market, he illegally sold P-1's to Iran, Libya, and North Korea…Another clue involves the United States. It obtained a cache of P-1's after Libya gave up its nuclear program in late 2003, and the machines were sent to the Oak Ridge National Laboratory in Tennessee, another arm of the Energy Department….Dr. Cohen said his sources told him that Israel succeeded – with great difficulty - in mastering the centrifuge technology. And the American expert in nuclear intelligence, who spoke on the condition of anonymity, said the Israelis used machines of the P-1 style to test the effectiveness of Stuxnet."

nuclear centrifuge control system to seize the opportunity to exploit cyber vulnerabilities when they became known in 2008. Intimate and nuanced knowledge of the terrain is not required to execute an effective attack in flat lands. However, intimate and nuanced knowledge of the terrain is required to effectively attack an enemy in the mountains, otherwise one could find oneself trapped in a valley, or accidentally outflanked, yielding advantage to the defender. Only with significant effort can such detailed intelligence of a complex environment leading to satisfactory orientation be gained in most instances, whether through deliberate advanced preparation as in the Stuxnet cyber attack, or through trial and error in the midst of battle like the Allies experienced at Monte-Cassino. The magnitude and patience of the intelligence and orientation effort essential to executing the Stuxnet cyber attack starkly brings into relief the complex, mountainous character of cyberspace.

Cyber Fortresses

In a complex environment, intelligence of the terrain is crucial, but so is how one uses the terrain to one's advantage, especially fortresses. Fortresses are simply artificial terrain features. While fortresses are useful means of preserving what resides within their walls for a time, the purpose of the fortress in defense since the Napoleonic era has been primarily to buy time for defensive reinforcements to arrive, as well as to weaken the attack. Fortresses weaken an attack by compelling the enemy to invest the fortress, and by attritting the attacking force to bring it to culmination more quickly. Additionally, fortresses fix an attack force in place making it vulnerable to a flank assault by forces dispatched from a supporting fortress. When fortesses are used accordingly, they often succeed, but when not, they typically fail. In 2007, Cyber Fortress Estonia was effective because it operated in accordance with these accepted lessons from land warfare, even if it succeeded by chance. Unfortunately, Georgia did not invest in similar cyber defensive preparations before the 2008 war with Russia.

Three historical examples from land warfare provide more recent demonstrations of the factors governing the success and failure of fortresses that Clausewitz aptly described more than 100 years ago. The US defense of the Pusan perimeter demonstrates successful use of a fortress to buy time for reinforcements to arrive, to attrit the enemy,

and use a flanking attack to crush an opponent. On the other hand, the French used fortresses, called *bases aero-terrestres* (air-ground bases), in Indochina, but failed to employ them effectively to culminate or annihilate their enemy.[35] Two examples of failing to employ fortresses properly are the French battles at Na San and at the infamous Dien Bien Phu.

Na San

At Na San, the French defense consisted of a series of dug in positions surrounded by barbed wire and minefields.[36] These were arranged to occupy a rough circle of hill tops about three miles across with an air strip at the center of the valley below.[37] Inside this outer ring, was an inner ring of continuous, entrenched strong points surrounding the air strip, the headquarters, medical station, stores, artillery and heavy mortar positions.[38] During the French build-up, a C-47 cargo plane landed every 10 minutes for at least six hours per day.[39] By the time Viet Minh forces first attacked on the night of 23 November 1952, the French fortress at Na San was formidable.[40]

The French artillery was devastating. Even with a numerical advantage of at least 10 to one, the Vietnamese could not dislodge a mere company of artillery-supported French Legionnaires from a hill top strong point.[41] French close air support and artillery helped make the strength of the Na San fortress formidable. Furthermore, a strong central reserve force was held in the fortress' center to quickly reinforce defenders at the point of attack.[42] So formidable was the fortress that Viet Minh forces retreated on 2 December 1952 in spite of their numerical superiority.[43]

On the surface, the French fortress at Na San appeared to have achieved its purpose, to preserve the force inside its boundary. However, the French failed to exploit

---

[35] Martin Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 1st Da Capo Press ed. (Cambridge, MA: Da Capo Press, 2004), 62.
[36] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 57.
[37] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 57.
[38] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 57.
[39] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 59.
[40] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 57-58.
[41] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 61.
[42] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 58.
[43] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 62.

the fortress' strategic value. With the Viet Minh forces fixed at Na San and other French strongholds free from enemy siege, the French failed to deploy reinforcements to execute a classic "hammer and anvil" strategy (to outflank and annihilate the enemy, in this case the Viet Minh) in a counterattack.[44] Although the French sent out strong patrols from Na San for several miles, they could not engage the retreating Viet Minh.[45] The French strategic error at Na San allowed the Viet Minh to avoid a decisive battle.

Some may argue that Na San was not a strategic failure for the French, because the battle weakened the Viet Minh through attrition. This argument would have merit only if the Viet Minh emerged weaker overall after the battle at Na San. The Viet Minh force gathered at Dien Bien Phu demonstrated the opposite; they learned from their experience at Na San to emerge even stronger.

Dien Bien Phu

According to Roman army historian Derek Williams, a military commander has two basic options in constructing an entrenched defensive position, the oyster or the peach.[46] Martin Windrow's summary of these defensive dispositions follows:

> The 'oyster' commits the bulk of the defenders to an outer shell of perimeter positions, dispersed between them according to a judgment of where the main attacks will fall. The perimeter may hold off the attackers for a long time, but if they manage to break through, then the soft interior, and the rear of the defensive perimeter, are at their mercy. The 'peach' defence spreads a relatively thin membrane around the outer edges to slow and weaken the attackers, but holds back most of its best assets in a central reserve. It accepts that attackers will break into the interior, though hopefully weakened by the resistance of the perimeter, and gambles on being able to destroy them by concentrating powerful reserves for a counter-attack when the direction of the threat has revealed itself. Choosing an effective balance between these approaches, governed by the ground and the available troops, is one of the fundamental skills of military command, whether the defenders are a company holding a hilltop or an entire army guarding a national frontier.[47]

---

[44] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 57-64.
[45] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 62.
[46] Williams cited in Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 302.
[47] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 302.

Unsaid in Windrow's description is that a fortress resembling an oyster is unlikely to survive against a *levee en masse* force without reinforcements from elsewhere to outflank and annihilate the enemy. Without external reinforcements from a supporting fortress, defenders of an oyster-type fortress are unlikely to ever have the advantage of concentric attack tactically or operationally. A fortress designed like a peach is perhaps more likely to survive a siege because it can better use interior lines to create a local advantage of concentric attack. Without reinforcements, a peach-type fortress will probably also fail like an oyster-type fortress to annihilate the enemy. Without external reinforcements from a supporting fortress, defenders of a peach-type fortress will probably never have the advantage of concentric attack operationally. With his lines of retreat secure, the enemy can escape and avoid annihilation. The French fortress at Na San was structured more like a peach. Na San survived, but without reinforcements to assume the advantage of concentric attack operationally, the Viet Minh escaped annihilation. The French fortress at Dien Bien Phu was constructed more like an oyster – it endured for a long time, but without reinforcements to outflank the Viet Minh, the result was disastrous.

The French garrison manning the air-ground fortress at Dien Bien Phu originally had orders to maintain free movement out to a five-mile radius from the air strip at the base's center.[48] Infantry were designated to hold the outer ring of fortifications while two paratroop battalions supported by artillery and heavy mortars made up the central reserve.[49] The perimeter positions were named Anne-Marie, Gabrielle, Beatrice, Isabelle, Dominique, Eliane, Claudine, and Huguette.[50] The French commanders assumed, erroneously, the defense would operate according to a peach model, similar to the fortress at Na San. The order to maintain freedom of movement to five miles dispersed the defensive perimeter's strong points such that the fortress tended to an oyster model; the defensive perimeter was too far out for the central reserve to successfully react and reinforce in a timely manner. Consequently, the infantry were ordered to hold their local strongpoints on the perimeter, supported by artillery, and make local counterattacks to recover temporarily lost ground, until the central reserve could launch an assumed

[48] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 303.
[49] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 303.
[50] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 15.

counterattack.[51] When this defense concept was put to the test, the French assumption proved false and Dien Bien Phu met with disaster.

The Viet Minh started the battle by attacking two of the strongpoints farthest from the center of the French defense, positions at hills the French called Beatrice and Gabrielle.[52] Beatrice fell first, followed by Gabrielle in two nights of fighting from 13 to 14 March 1953.[53] On the morning of 15 March, the commander of the French garrison at Dien Bien Phu decided to launch a counterattack using the central reserve to re-take Gabrielle.[54] The counterattacking reserve had to cover two miles of open terrain before reaching Gabrielle, much farther than the reserve had to travel at Na San.[55] In addition, the reserve had to traverse that ground under whithering Viet Minh artillery fire, a hazard not present at Na San.[56] Consequently, the central reserve proved useless as a counterattack unit to reinforce the perimeter strongpoints at Dien Bien Phu. This French miscalculation denied the defenders the ability to use interior lines to generate the tactical advantage of concentric attack as they did at Na San. Still, Dien Bien Phu proved exceptionally strong, attritting the Viet Minh and prolonging the battle. Unfortunately, the French did not exploit this strength to seize the concentric attack advantage by deploying reinforcements to encircle and destroy the Viet Minh engaged at Dien Bien Phu.

As previously described, the *levee en masse* assures that a committed adversary can siege and defeat a fortress with sufficient time; Dien Bien Phu was no exception. For six weeks, the French garrison, representing less than four percent of total forces available, managed to tie down about 60 percent of Viet Minh regular forces, 20 percent of their total in Indochina.[57] Of those, the Viet Minh forces laying siege to the French

---

[51] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 303.

[52] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 378-79, 97. "In the main position either Beatrice or Gabrielle were the obvious first choices for the assault phase: they were the furthest from French support, the nearest to the Viet Minh's direction of approach, and they barred the way to any concentration of People's Army artillery and [anti-aircraft] guns closer to the airfield." Shortly before 1720 hours on 13 March 1953, the first Viet Minh shells fell on Beatrice. On the night of 14 March the Viet Minh assault on Gabrielle started.

[53] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 378-403.

[54] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 403.

[55] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 403, 09.

[56] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 409.

[57] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 539-40.

fortress suffered almost 50 percent casualties.[58] Used in the manner Clausewitz described, the Dien Bien Phu fortress presented a golden opportunity for the French to deal a crushing blow to the Viet Minh armed forces, perhaps even a decisive defeat. The French failed to seize the moment, unable to match even the limited victory they achieved at Na San. Although token French reinforcements were eventually dispatched their numbers and quality were insufficient to turn the tide in the French's favor.[59] The French did not abide by the hard lessons of others' war experience, for myriad reasons, in their use of the fortress at Dien Bien Phu. The end was a humiliating defeat for the French and a decision for the Viet Minh. After the debacle of Dien Bien Phu, the French withdrew from Indochina.

Fortress Pusan

The French use of fortresses in Indochina was unsuccessful because they did not employ their fortifications to maximum strategic advantage. The French did not use the fortress to accomplish the following strategic tasks: to change the balance of forces through enemy attrition, to buy time in order to change the balance of forces with reinforcements, and to seize the advantage of concentric attack by using reinforcements to outflank an enemy fixed by the fortress. Three years prior to the battle of Dien Bien Phu, American forces in the Korean War took refuge inside the Pusan perimeter, Fortress Pusan, and used the fortress to maximum advantage.

On 25 June 1950, the North Korean People's Army (NKPA) invaded the Republic of Korea (ROK) in the south.[60] ROK forces and their American compatriots were immediately on their heels. By 10 July 1950, the US commander, General Douglas MacArthur, had laid out his plan to outflank the NKPA at Inchon.[61] To execute his plan,

[58] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 539.
[59] Windrow, *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*, 578.
[60] Conrad C. Crane, *American Airpower Strategy in Korea, 1950-1953*, Modern War Studies (Lawrence, KS: University Press of Kansas, 2000), 1.
[61] Bill Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 1st Simon & Schuster hardcover ed. (New York, NY: Simon & Schuster, 2009), 46-47.

General MacArthur requested that the entire 1st Marine Division deploy to Korea with an arrival date no later than 2 August 1950.[62]

In order to pull off MacArthur's plan, ROK forces and the US 8th Army needed to stave off defeat until the reinforcements arrived. They fought a valiant retrograde against the NKPA until they could fall back no farther. If the port of Pusan fell, reinforcements could not easily land on the Korean peninsula. When the 8th Army retreated across the Naktang River on 31 July 1950, their commander, General Walton Walker, ordered them to make a stand or else – to fight to the end.[63] It was then that the Naktang River became virtually synonymous with the Pusan Perimeter.[64] Fortress Pusan was born.

Fortunately, the 8th Army's defense bought enough time for reinforcements to arrive at Pusan. The first elements of the 1st Provisional Marine Brigade reached Pusan on 1 August 1950, with most of the remaining Marine force arriving in port the following day.[65] Almost immediately, the Marine reinforcements were used for local counterattacks to thwart NKPA assaults on the perimeter, similar to the way the French used their central reserve at Na San and tried to use their reserve at Dien Bien Phu.[66] For example, a Marine counterattack at Chindong-Ni turned a near disaster into an enemy rout. The Marines launched the counterattack on 7 August after an NKPA assault threatened to cut the Masan road supply line from the port to forces manning the Pusan perimeter.[67] Known in Marine Corps history as the Kosong Turkey Shoot, Chindong-Ni was the first time in the war that the NKPA had been forced into general withdrawal.[68]

---

[62] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 47.
[63] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 84.
[64] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 65.
[65] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 86-87.
[66] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 123.
[67] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 123.
[68] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 123-25.

Try as they might, the NKPA never broke through Fortress Pusan. Marine reinforcements used as a reserve to counterattack at the point of NKPA assaults repeatedly kept the perimeter intact and bought time for the Inchon landing force to arrive and organize. Simultaneously, the NKPA strength was decreasing through attrition. Of the 10 NKPA divisions that originally laid siege to the Pusan Perimeter, one division was shattered and parts of four others had been badly defeated.[69] By the end of the Second Battle of Naktang on 6 September 1950, Fortress Pusan had fulfilled two of its strategic functions.[70] The fortress had changed the balance of forces through attrition. The US fortress also bought time for reinforcements to arrive and decisively alter the balance of forces.

On 15 September 1950, the Pusan Perimeter fulfilled the third strategic function of a fortress – it fixed the NKPA force so that American reinforcements could execute a decisive flank attack.[71] On that day, the Marines made their famous landing at Inchon at 0655L, finding virtually no enemy resistance.[72] Having used their fortress to change the balance of strength in their favor, US forces seized the advantages of initiative, surprise, and concentric attack to rout the NKPA, which barely escaped total annihilation. Only Chinese intervention saved Korea from being unified under the ROK flag.

Cyber Fortress Estonia

Fortuitously, during the cyber conflict of 2007 Estonia used its cyber fortress in a manner similar to the Americans at Pusan in the Korean War, rather than the French in Indochina. The Estonians used their cyber fortress to weaken the attack, to buy time and secure reinforcements, and ultimately to outflank the enemy in a counterattack.

---

[69] Sloan, *The Darkest Summer : Pusan and Inchon 1950 : The Battles That Saved South Korea--and the Marines--from Extinction*, 85, 166, 188, 209. In the First Battle of Naktang, one NKPA division was destroyed in what is known as the Kosong Turkey Shoot in the US Marine Corps. In the Second Battle of Naktang, an assault by parts of four NKPA divisions was defeated.

[70] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 209.

[71] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 228. Robert Debs Heinl, Jr., *Victory at High Tide: The Inchon-Seoul Campaign*, Great War Stories, 3rd ed. (1979; repr., Charleston, SC: The Nautical and Aviation Publishing Company of America, 2002), 41. The bulk of the NKPA were committed against the Pusan Perimeter.

[72] Sloan, *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*, 232.

When the distributed denial of service (DDoS) cyber attack against Estonian websites and servers started on 26 April 2007, the first response was to take refuge behind a virtual castle wall. Since the cyber attacks were launched from botnets and cyber militia computers outside Estonia, cyber defenders simply raised the virtual drawbridge and shut down access to Estonian websites from abroad.[73] The attackers maneuvered around these walls to a degree by activating botnets composed of hijacked computers inside Estonia, as well as by using sympathetic ethnic Russian cyber militiamen inside the country to continue the barrage.[74] Even though the Estonian cyber fortress did not defeat the cyber attack, it weakened the assault force by limiting the number of attack computers. Cyber Fortress Estonia served one strategic purpose by weakening the cyber attack's potential strength.

Estonia's cyber fortress also bought the state time to secure reinforcements in the form of additional network server capacity, filters to screen out cyber attack network traffic, and allies. The director of the Estonian Computer Emergency Response Team, Hillar Aarelaid, was fortunate to have dinner with a member of the Vetted, Kurtis Lindqvist, four days after raising the virtual drawbridge.[75] Lindqvist and two other members of the Vetted were in Estonia for a conference at the time of the cyber attacks by mere happenstance.[76] These were three of a handful of people in the world trusted by the globe's largest Internet Service Providers (ISPs) to remove rogue computers from the network.[77] With additional server capacity and filters to weaken the cyber attack when the virtual draw bridge lowered, as well as allied forces, the Vetted, who could out flank the attackers, Aarelaid and his team had shifted the balance of forces in favor of their cyber defense. Fixed on breaking through Estonia's cyber fortress, the cyber attackers were vulnerable to a classic flank attack.

[73] Ruus, "Cyber War I: Estonia Attacked from Russia." Davis, "Hackers Take Down the Most Wired Country in Europe."

[74] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24. Evron and Aarleid, "Estonia: Information Warfare and Lessons Learned," 17. Rosanna E. Guadagno, Robert B. Cialdini, and Gadi Evron, "Storming the Servers: A Social Psychological Analysis of the First Internet War," *Cyberpsychology, Behavior, and Social Networking* 13, no. 4 (2010): 450. Existing evidence suggests that some of the ethnic Russians who participated in the cyber attacks were living in Estonia.

[75] Davis, "Hackers Take Down the Most Wired Country in Europe."

[76] Davis, "Hackers Take Down the Most Wired Country in Europe."

[77] Davis, "Hackers Take Down the Most Wired Country in Europe."

When the last major cyber onslaught struck Estonia at midnight on 9 May 2007, Estonia's cyber defenders were prepared to seize the initiative and concentric attack advantages in a counterattack.[78] Aarelaid and his team traced the origin of the attacks to specific computers, and passed their virtual positions to his three Vetted allies who sent e-mails to the ISPs to excise the attacking computers from the Internet at the source.[79] Estonia's Internet traffic hovered just above normal by morning, never being overwhelmed.[80] Estonia's cyber defense used a classic flank attack to succeed. Estonia's cyber defense cut off the essential lines of communication between the source of supply (the attack computers) and the attack force (the attack data packets) at the point of attack (the target websites and servers).

Cyber Fortress Estonia served to facilitate a shift of strategic advantage to the defense in a manner congruent with the theory and experience of land warfare. Estonia's cyber fortress weakened the enemy, bought time to secure reinforcements, and helped fix the adversary's force so that it was vulnerable to a flank counterattack on enemy lines of communication. Like Fortress Pusan in 1950, Cyber Fortress Estonia helped swing initiative and concentric attack, two determinants of advantage in strategy, in favor of the defense. However, Estonia's defensive success on 9 May 2007 did not produce a decision, since cyber attacks continued at lower levels for nine more days.[81]

The lack of a decision from the Estonian cyber counterattack owes primarily to two distinct characteristics of cyberspace – reparability resulting from artificiality, and concealment derived from uncertainty of human attribution inherent in the domain. Concealment in particular prevented Estonia's counterattack from achieving a decision because the counterattack could not locate and eliminate the true source of the cyber attack, the humans who were the ultimate masters of the hostile computer army.

---

[78] Davis, "Hackers Take Down the Most Wired Country in Europe."
[79] Davis, "Hackers Take Down the Most Wired Country in Europe."
[80] Davis, "Hackers Take Down the Most Wired Country in Europe."
[81] Davis, "Hackers Take Down the Most Wired Country in Europe."

CHAPTER 5

CONCEALMENT AND PERSISTENCE IN SEA AND CYBER POWER

The key similarity between sea and cyber power is the ability to conceal persistent strength. This ability in both the sea and cyberspace creates advantages in war. Concealment helps give the side possessing it the advantage of initiative and surprise, because concealment changes the speed ratio of intelligence to preparation to near unity. Survivability of the force also rises with the ability to conceal, boosting the capacity of that force to exploit moral factors to their advantage. To augment these advantages, the capability to conceal persistent striking power leads to a superior ability to apply concentric attack, as well as to retain the initiative, despite relatively long attack mobilization times.

In sea power today, only submarines possess the combination of persistence and concealment from which these warfare advantages in concentric attack, initiative, and the exploitation of moral factors derive. The development of stealthy surface ships may change this situation in the future, but up to now only submarines have benefited from the combination of these qualities in sea warfare. In cyber power, like submarine warfare, concealment and persistence are corporeal, flowing from the nature of cyberspace itself.

The Battle of the Atlantic and the US submarine war against Japan in World War II (WWII), as the two most recent instances of large-scale submarine warfare, bring the elements of concealment and persistence in sea power into focus. Similarly, the Estonian and Georgian cyber conflicts of 2007 and 2008 highlight the advantages of initiative, concentric attack, and moral factors, which flow from the synergy of concealment and persistence.

Submarine Warfare in World War II

The Battle of Japan put the Allies in the hunter role, with US submarines attacking Japanese shipping to choke the import-dependent Japan into submission.

However, the most feared sea hunters roamed throughout the Battle of the Atlantic from 1939 to 1941, as German submarines organized into wolf packs targeted Allied convoys. These convoys were the British life-blood of supplies and war material from the United States. Without the convoys, the Allies feared Britain would fall.

The Battle of the Atlantic

The first German U-Boats (submarines) deployed in individual patrols when almost all Allied merchant ships traveled singly.[1] When the Allies brought convoys into full swing during October 1939, Admiral Karl Donitz, Commander of Submarines of the *Kriegsmarine* (the German Navy), altered his strategy.[2] He deployed two groups of 10 U-Boats, also known as wolf packs, to hunt Allied convoys in the Atlantic.[3] The first wolf pack deployment failed to generate significant Allied losses, but Donitz and his submarine force learned from their mistakes.

The new U-Boat wolf pack strategy and tactics took maximum stock of the submarine's concealment and persistence. Initially, the wolf packs were guided by intelligence gathered from breaking Allied codes, but Allied anti-submarine air and surface patrols forced the wolf packs westward, away from British shores and into the great expanse of the Atlantic Ocean.[4] This forced the wolf packs to adopt tactics that would allow them to cover large areas.[5] Therefore once deployed, a wolf pack would disperse into a patrol line, with about 15 miles spacing in between each boat in the line.[6] A typical pack of 12 U-Boats could span an area 165 miles across.[7] When the first U-Boat made contact with an Allied convoy, the submarine was to shadow the convoy and

[1] Blair, Clay, Jr., *Hitler's U-Boat War: The Hunters 1939-1942* (New York, NY: Random House, 1986), 110.

[2] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 110. Allied convoys started in earnest in October 1939, which sparked the Germans to start their wolf pack strategy. John Keegan, *Battle at Sea: From Man-of-War to Submarine*, Pimlico ed. (London, UK: Pimlico, 1988). Hitler appointed Admiral Karl Donitz, a veteran of the World War I unrestricted submarine campaign, commander of the U-Boat fleet in 1935.

[3] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 110.

[4] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 110, 423.

[5] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 423.

[6] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 423.

[7] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 423.

transmit a beacon signal for the other submarines in the pack to converge upon it.[8] It could take up to an hour for the next member of the wolf pack to make contact with the target convoy, given these U-Boats could only cruise at 15 to 20 knots on the surface and half that submerged.[9] Hence, it was difficult for the most distant U-Boats to reach the target convoy because the pack's mobility was hampered by the beacon submarine's vulnerability to being located by radio triangulation before the pack could concentrate.[10] Additionally, if the U-Boats detected Allied anti-submarine air power, they would submerge, reducing their speed and delaying their arrival upon the detected convoy.[11] Once all U-Boats had concentrated upon the target, they were to attack in a single, simultaneous blow, scattering the convoy and overwhelming the escorts.[12] This approach maximized the opportunity for repeated attacks on a disaggregated and disintegrated opponent while minimizing the opportunity for Allied counterattacks.[13] Even with the long time required for the dispersed U-Boats to converge, the submarine's concealment and persistence made the wolf pack strategy possible and highly effective.

The U-Boat's concealment allowed the beacon submarine to remain in contact with a convoy despite the local balance of forces favoring the convoy if an engagement were to occur. If possible, a convoy would have preferred an engagement against this lone U-Boat because destroying it would eliminate the homing beacon drawing in the rest of the wolf pack. However, concealment combined with persistence allowed the beacon U-Boat to refuse battle and wait the long duration it took for the pack to concentrate. The pack could then attack the target convoy on multiple flanks, because concealment allowed the pack to maneuver around the convoy unseen, positioning the submarines to exploit the advantage of concentric attack when they pounced. Lastly, the submarine's concealment conferred the advantage of initiative and surprise to the wolf pack. Concealment permitted the pack to engage the convoy under conditions of the pack's choosing, while simultaneously driving the speed ratio of intelligence to preparation to

8 Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 114. Keegan, *Battle at Sea: From Man-of-War to Submarine*¸ 235-36. Radio availability was also required because U-Boat headquarters designated patrol positions and directed to maneuvers against convoys when U-Boats spotted them.

9 Keegan, *Battle at Sea: From Man-of-War to Submarine,* 234-35.

10 Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 423.

11 Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 423.

12 Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 114.

13 Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 114.

one, denying the convoy any reaction time – it typically only knew it was under attack when it absorbed the first blow.

Concealment also yielded a moral advantage to the German wolf packs, allowing them to act with a level of boldness that would otherwise have been foolhardy. For example, a small force of 25 U-Boats traveled thousands of miles to hostile US waters in January 1942.[14] That wolf pack sank 71 Allied convoy ships (401,000 tons), including 23 oil tankers.[15] Despite being in the heart of enemy territory, all of these U-Boats, save one, escaped to fight another day.[16] The moral advantage conferred by their high survivability, which itself flowed from the U-Boat's concealment, supported the boldness necessary to launch this attack deep within enemy territory using such a small attack force. This attack demonstrated true strategic daring, given that it took the force weeks, if not months, to return to the safety of German waters after ambushing this Allied convoy.

The wolf pack attack off the American coast was a microcosm of the German U-Boat campaign's grossly lopsided results. In the first 28 months of the war, Germany deployed 153 oceangoing attack submarines.[17] During that period, U-Boats sank 1,094 merchant vessels and 28 warships, 5.3 million gross tons of shipping.[18] Germany lost just 49 of their 153 submarines in the Battle of the Atlantic to that point for an impressive kill ratio of almost 23 to one.[19] German submarine warfare slashed British imports nearly in half from 1939 to 1941, from 60 million to 31 million tons.[20] In terms of results, U-Boat wolf packs, harnessing the advantages they gained from exploiting concealment and persistence, attacked with devastating efficiency and effect.

Only breaking the German Enigma code-machine enabled Allied convoys to successfully evade the U-Boat wolf packs.[21] Avoiding U-Boat patrol areas deprived the wolf packs of the opportunity to use their advantages of initiative/surprise and concentric

[14] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 508.
[15] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 508.
[16] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 508.
[17] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 418.
[18] V.E. Tarrant quoted in Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 418.
[19] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 419.
[20] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 419.
[21] Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 421.

attack against the convoys. The German wolf packs were patrolling in the wrong areas. As a result of Allied code-breaking and their subsequent orientation advantage, U-Boats could not employ their superiority in initiative and concentric attack for success in the Battle of the Atlantic. As it turned out, Allied code-breaking also significantly influenced the effectiveness of sea power in the Pacific.

The Submarine War in the Pacific

Submarine warfare was also prominent in the US war in the Pacific, but differed from the Battle of the Atlantic because both the United States and Japan, depended on sea power to sustain and execute their war efforts. The American island hopping campaign rested upon the ability to seize new island bases by amphibious assault, and to supply those forward base areas by sea. The Japanese home islands and military, like the British, depended on imports from abroad, transported by sea, for their survival. Accordingly, the United States and Japan both attempted to engage in a *guerre de course*, sea interdiction, using submarine warfare.

It took American submariners in the Pacific a long time to absorb lessons from their experience with German wolf packs in the Atlantic that could have been implemented to US benefit much sooner. The US submarine campaign against Japanese shipping could have benefited from lessons learned during two years of fighting in the Battle of the Atlantic. Yet, the US submarine command in the Pacific did not immediately adopt a similar strategy to the Germans despite success of U-Boat wolf packs. The Americans failed to deploy a submarine wolf pack in the Pacific until October 1943, almost two full years after the start of the war with Japan.[22]

The US Navy adopted a slightly modified version of the German wolf pack tactics. First, American wolf packs only consisted of three submarines compared with 10 to 12 for the Germans.[23] Once one of these US submarine spotted a Japanese convoy, like the Germans, the submarine would transmit the convoy's position to the other

[22] Blair, Clay, Jr., *Silent Victory: The U.S. Submarine War against Japan* (Philadelphia, PA: J. B. Lippincott Company, 1975), 543.

[23] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 542. Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 110, 423.

submarines via short-range radio.[24] However, to avoid being vulnerable to Japanese triangulation, the US submarine would not broadcast a signal beacon like the Germans had. This emphasis on radio discipline for survivability led to communication and navigation problems that made executing a well coordinated wolf pack attack difficult.[25] Furthermore, unlike the Germans, the American packs did not plan to attack simultaneously for fear of fratricide.[26] Instead, the first ship would attack and then drop behind to trail the convoy and finish off any stragglers.[27] The other two submarines would then take up position on the port and starboard flanks of the convoy, alternating attacks, hoping one attack would turn the convoy toward the other submarine waiting to pounce.[28] The Allied orientation advantage gained from code-breaking explains how the US Navy could employ German wolf pack tactics with three submarines instead of 10 or 12. In the Pacific, American Ultra code-breaking intelligence provided Japanese convoy sailing dates and routes that allowed US submarines to lie in wait at choke points like the Luzon Strait.[29] Therefore, since American wolf packs did not have to cover the same large ocean areas as U-Boat packs, US submarines could operate in smaller groups. Even with the strategic advantage in orientation rendered by Ultra, the first US wolf packs did not sink many ships.[30]

George Edmund Peterson led the first successful American wolf pack in March 1944.[31] He had spent most of WWII to that point operating in the Atlantic out of Scotland.[32] Peterson developed new, simplified techniques to facilitate communications.[33] He combined the effectiveness of the German signal beacon, which he observed firsthand during the Battle of the Atlantic, while mitigating the beacon method's vulnerability to enemy radio direction finding. According to Peterson's communication system, the first submarine sighting a convoy would surface, provide a

---

[24] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 542. Blair, *Hitler's U-Boat War: The Hunters 1939-1942*, 114.
[25] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 542.
[26] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 542.
[27] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 542.
[28] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 542.
[29] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 597, 692.
[30] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 542-51.
[31] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 597.
[32] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 597.
[33] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 597.

contact report to the rest of the pack, and continue this reporting every hour.[34] This system provided regular rendezvous guidance for the rest of the pack while reducing the risk of the Japanese detecting the shadowing American submarine. Using this communications technique and the convoy attack tactics previously described, Peterson's wolf pack sunk five vessels out of a 12-ship convoy on their first patrol.[35]

In 1944, the perfected wolf pack tactics led the United States to a rout over Japan in the submarine war in the Pacific.[36] That year, American submarines sank 603 ships, 2.7 million tons, more than the previous two years combined.[37] Japan's bulk commodity imports fell from 19.4 million tons at the end of 1942, to 16.4 million tons at the end of 1943, to just 10 million tons by the end of 1944.[38] In addition, the flow of oil to the Japanese home islands from the southern regions of the Pacific nearly ceased, to the point Japanese leaders launched experiments to conjure oil from potatoes.[39] Lastly, the US Navy decimated the Japanese submarine fleet and rendered it ineffective. The Japanese submarine fleet lost 56 boats in 1944 compared to just 19 American submarines losses.[40] Moreover, Japanese submarines achieved nothing of note in their attempts to stop the invasions of the Marshall, Marianas, Palaus, or Philippine island chains.[41]

The American submarine wolf packs' combination of concealment and persistence, combined with tactics similar to the U-Boat wolf packs, yielded the same advantages of initiative, surprise, and concentric attack that the Germans enjoyed in the Battle of the Atlantic via similar mechanisms. Concealment also created a strategic advantage in the exploitation of moral factors similar to the one the German submarine force enjoyed before the Allies broke their Enigma codes. Concealment increased the survivability of the US submarine force, supporting the boldness and daring necessary to pursue a strategy of small group operations, wolf packs of just three submarines, far from

---

[34] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 597.

[35] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 597-99.

[36] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 819. For all practical purposes the US submarine war against Japan was over by December 1944.

[37] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 816. From the end of 1941 through 1943, US submarines sank 515 ships, a tonnage of 2.2 million.

[38] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 522, 816.

[39] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 816.

[40] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 816-18.

[41] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 818.

the safety of US home waters. Ultra intelligence, combined with the submarine's inherent characteristics, significantly enlarged the US submarine force's strategic advantage in the exploitation of moral factors.

The US submarines' increased survivability, initiative, and concentric attack advantages created by their concealment and persistence, and their orientation advantage produced by Ultra intelligence, combined to generate a cadre of Japanese merchant seamen who feared leaving Japanese home waters because their convoys would almost inevitably be attacked and perhaps lead to a terrifying death at sea.[42] These convoys faced near certain attack due to Ultra intelligence. Ultra oriented the American submarine force so that it could lay in wait for Japanese convoys.[43] Without espionage activity like Ultra to seize the orientation advantage or a reliable means of observation to detect US attack submarines, Japanese seamen knew that their convoy defense measures were futile. Consequently, the seamen calculated that the cost of running a convoy outside Japanese home waters would certainly be high. These Japanese convoys also lacked reliable means to increase their probability of success. When people believe that their action will have little probability of succeeding and expect to produce nearly zero benefits, they will generally not try to take that action.[44] This hesitancy to act increases when the costs associated with attempting such a fruitless endeavor are certain and high.[45] For example, when two US wolf packs attacked a convoy leaving Formosa headed for the Philippines on 17 August 1944, they sank three ships and damaged four others.[46] The surviving Japanese ships scattered and returned to Formosa.[47] No supplies reached the Philippines in this instance.[48] The convoy's refusal to proceed illustrates how US advantages in orientation, initiative, and concentric attack meshed to produce an American advantage in the exploitation of moral factors – fear in the hearts of Japanese merchant seamen.[49] Japan simply *stopped trying* to send convoys outside Japanese home

[42] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 688.
[43] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 692.
[44] Robert A. Pape, *Bombing to Win: Air Power and Coercion in War*, Cornell studies in political economy (Ithaca, NY: Cornell University Press, 1996), 17.
[45] Pape, *Bombing to Win: Air Power and Coercion in War*, 17.
[46] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 706-07.
[47] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 706-07.
[48] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 706-07.
[49] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 688.

waters in spite of having more than 2.8 million tons of available shipping capacity at the end of 1944.[50]

In summary, the US submarine war against Japan exhibited several similarities to the German U-Boat campaign. These similarities were in how the submarine's inherent qualities of concealment and persistence combined to produce advantages in initiative and concentric attack, as well as in exploiting moral factors to support more daring strategies. The synergism of these advantages and the American orientation advantage derived from code-breaking intelligence birthed an even grander margin for the United States in the exploitation of moral factors than the Germans possessed in the Battle of the Atlantic. This margin expressed itself as Japanese fear, and as a sense of futility in trying to convoy beyond Japanese home waters.[51] The advantage in moral factors effectively ended the American war on Japanese shipping in December 1944 although Japan retained significant shipping capacity.[52] Except orientation, all of the American advantages in strategy emanated from the submarine's innate qualities of concealment and persistence, qualities also inherent to cyber power as evident in the Estonian and Georgian cyber conflicts.

Concealment and Persistence – Effect on the Estonia and Georgia Cyber Conflicts

Concealment and persistence are inherent to cyber power. The effect of these qualities on the Estonian and Georgian cyber conflicts resulted in dynamics similar to those observed in WWII submarine warfare – advantages in initiative and surprise, concentric attack, and the exploitation of moral factors.

In the Estonia and Georgia cyber conflicts of 2007 and 2008, the most clearly visible effect of cyber power's quality of concealment was in the exploitation of moral factors, which manifested in the ease, speed, and make-up of the attacking, all-volunteer, cyber militias. In the Estonian conflict, the cyber attackers recruited the volunteer, amateur force, which likely approached 100 thousand or more members, by posting the equivalent of an army recruiting pitch in Russian-language chat rooms over a five-day

[50] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 816-19.
[51] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 692, 706-07, 819.
[52] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 819.

period.[53] The size of the cyber militia involved in Georgia's 2008 cyber conflict was much greater than the one that engaged Estonia. Both cyber militias were organized in Russian-language Internet forums during a brief timeframe.[54] It would be virtually impossible to raise an all-volunteer land army in the tens or hundreds of thousands so quickly absent a threat to national survival. The concealment offered by cyber power provided so much protection from reprisal, was so morally empowering, that the cyber attackers gathered armies of amateur cyber warriors that literally included children.[55]

The easiest way to comprehend the degree of survivability created by cyber power's inherent quality of concealment is to compare the number of cyber militia attackers in both conflicts arrested to the number of physical rioters arrested in just the Estonian incident. Of the almost 100,000 or more cyber militiamen involved in the cyber attacks on Estonia and Georgia across multiple countries, only one man was arrested.[56] However, the physical riots in Estonia resulted in one death, more than 100 injuries, and almost 1,000 arrests from a group of rioters that numbered in the thousands.[57] Those who took part in the physical riots had a more than 10 percent chance of suffering immediate, negative consequences. The cyber militiamen who attacked Georgia and Estonia, on the other hand, faced an insignificant 0.00001 percent chance of being punished. The cyber militiamen could act with virtual impunity.

---

[53] Davis, "Hackers Take Down the Most Wired Country in Europe." One week after the statue was moved on 27 Apr 2007, on or about 4 May, posts in Russian-language Internet forums called for a coordinated cyber strike against Estonia on 9 May. The attacks on 9 May consisted of more than one million computers (botnet size ranged in the hundreds of thousands of computers). The difference in botnet size and the attack's overall size suggests 100,000 cyber militiamen is a reasonable estimate.

[54] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4. Evron and Aarleid, "Estonia: Information Warfare and Lessons Learned," 6, 18. Russian-language Internet forums were updated periodically with instructions and targets.

[55] Aareleid quoted in Urmas Vahe, "On the Front Lines of an Invisible War," *Baltic IT&T Review*, http://www.ebaltics.com/00704599?PHPSESSID=8b81c5fl58bb827ald825148e4d07c54 (accessed 31 May 2011). "Lots of attack[s] were launched from the computers of Russian speaking schoolboys in Estonia."

[56] "Estonia fines man for 'cyber war'," *BBC News*, 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm (accessed 3 April 2011). Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, 4 April 2009, http://www.iar-gwu.org/node/65 (accessed 3 April 2011).

[57] Luke Harding, "Protests by Kremlin as police quell riots in Estonia," *Guardian: The Observer*, 29 April 2007, http://www.guardian.co.uk/world/2007/apr/29/russia.lukeharding (accessed 3 April 2011). Ben Nimmo, "Violence rocks Estonia as riots spread beyond Tallin," *M&C News.com*, http://www.monstersandcritics.com/news/europe/news/article_1297586.php/Violence_rocks_Estonia_as_riots_spread_beyond_Tallinn (accessed 3 April 2011).

It obviously takes far less courage to strike when one is nearly guaranteed immunity. The moral advantage that American and German submarine forces derived from concealment was magnified greatly for these cyber attackers. This moral advantage facilitated not just strategic daring, but a *levee en masse*. Cyber power's natural quality of concealment provided the ultimate masterminds of the cyber attacks the ability to exploit moral factors to their advantage by nearly eliminating the necessity for participants to possess any strand of physical courage in the Estonia and Georgia cyber conflicts. As a result, the organizers of the attacks were able to raise massive cyber militias, a virtual *levee en masse*. These *levees en masses* allowed the cyber militias to attempt with cyber power what would have amounted to all out civil war had similar disruption been attempted using land power. Cyber power's concealment and persistence also expressed themselves in the form of initiative and concentric attack advantages, similar to the advantages held by US and German wolf packs in WWII. As the submarine's initiative advantage allowed the ship strike without warning in WWII, cyber power hit with surprise in Estonia in 2007. The botnets used in the cyber attacks on Estonia were composed of zombies, computers hijacked by malicious Trojan-horse software, that were centrally controlled.[58] Many of these zombies were concealed inside Estonia. The ability of the malicious software to persist, concealed inside Estonian computers granted the cyber attackers the initiative to strike at the most opportune moment. That moment arrived when Estonia cut off its international Internet connections and took refuge within Cyber Fortress Estonia. The botnets concealed within Estonia pounced in a surprise attack that temporarily negated the advantages of an Estonian cyber fortress.[59]

The botnet attack from within Cyber Fortress Estonia also illustrates the concentric attack advantage the cyber attackers enjoyed resulting from persistent concealment in cyberspace. When Estonia cut off its international Internet connections, the country effectively defined a defensive cyber front toward which its defenses were directed. The botnets concealed within Estonia allowed the cyber attackers to outflank

[58] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.

[59] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.

this defensive barrier, such that the attackers could rise from within Estonia's defensive perimeter, like saboteurs but with greater mass. The zombies in Estonia allowed the attackers to engage Estonia's cyber defenses from the front and rear simultaneously.

Additionally, in the case of Georgia, the cyber attackers' advantages in concentric attack, initiative, and survivability appear to have been so overwhelming that some cyber defenders made no effort to mitigate the attack.[60] Like the Japanese merchant seamen who turned back at Formosa in WWII, some Georgian cyber entities made no effort to defend themselves when they were under assault, even though they could have tried. One possible inference from the actions of these cyber actors in Georgia is that faced with a low probability of success, they were coerced not to put forth the effort to even mount a token cyber defense.

Lastly, long attack mobilization times are needed to overcome the complex cyber terrain. In WWII, concentrating submarine wolf packs after a target convoy was sighted also took a long time. Such long mobilization times would have been suicidal, but the submarine's ability to remain concealed for an extended period allowed these wolf packs to retain the initiative. For example, it is unfathomable to believe a convoy's escorts would have let an easily observable, enemy surface ship shadow the convoy for hours or days it while the enemy ship awaited reinforcements. Only the submarine's persistent concealment made this possible. Similarly, only cyber power's persistent concealment allowed the cyber attackers to survive, to refuse an engagement on unfavorable terms and to avoid provoking Estonia and Georgia to prepare or deploy stronger cyber defenses, while the attackers gathered the necessary cyber intelligence for their assaults. The cyber attackers in Georgia and Estonia must have gathered some cyber intelligence in advance of the conflicts without the cyber defenders' knowledge because the attacks came without any observable intelligence gathering stages and some of the cyber assaults targeted very specific vulnerabilities.[61] Consequently, cyber power's inherent concealment afforded

---

[60] Shadowserver quoted in Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14. "[S]ome of the attacked websites remained online and did not really make any changes to defend themselves."

[61] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4-5. Evron and Aarleid, "Estonia: Information Warfare and Lessons Learned," 18.

the attackers an initiative advantage notwithstanding the long attack preparation time presumably involved.

The Estonian and Georgian cyber conflicts illustrate the similarities between cyber power and the submarine in sea power to leverage their inherent properties of persistence and concealment for advantage in war. Cyber power's quality of concealed, persistent striking power created advantages of initiative and surprise, concentric attack, and the exploitation of moral factors. However, this initiative advantage depended upon intelligence, knowing the very complex cyber terrain. That the initiative advantage hinges on advanced preparation using intelligence is a feature of cyber power that is better highlighted through its similarities to air power.

CHAPTER 6

SPEED, MOBILITY, AND INTELLIGENCE IN AIR AND CYBER POWER

Cyber power shares similarities with land and sea power, and to air power as well. Both cyber and air power have a speed of action greater than that possible in the traditional warfighting domains that preceded their use. Both possess the mobility to circumvent an adversary's fielded forces to strike at otherwise protected enemy lines of communication and the heart of enemy power from a conflict's start. Lastly, effective use of both air power and cyber power relies on extensive intelligence preparation of the battlespace.

Speed is the main quality shared between air and cyber power, not absolute speed, but the impact of speed inherent in these two forms of power on the relative quantity of the speed ratio of intelligence to preparation, from which the initiative advantage flows.[1] During the Interwar Years, air power theorist Giulio Douhet articulated the primacy and advantage of the offensive in air warfare.[2] At the time of Douhet's writing, attack held the advantage over defense in air warfare because there was no way to observe an air attack with sufficient accuracy and warning time to mount an effective defense.[3] The

[1] Corbett, *Some Principles of Maritime Strategy*, 259. As the speed ratio of intelligence to preparation decreases, the chance of surprise increases.

[2] Giulio Douhet, *The Command of the Air*, ed. Joseph Patrick Harahan and Richard H. Kohn (Tuscaloosa, AL: University of Alabama Press, 1998), 55. "[A]erial warfare admits of no defense, only offense. We must therefore resign ourselves to the offensives the enemy inflicts upon us, while striving to put all our resources to work to inflict even heavier ones upon him."

[3] Douhet, *The Command of the Air*, 49-50. "The attack may therefore be prepared in complete secrecy and launched without forewarning the enemy, with the offensive retaining advantages of operational initiative. And, considering the suddenness of the attack, it is unlikely that the enemy would have time enough to parry the blow effectively either in the air or from the ground." William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military* (Tuscaloosa, AL: University of Alabama Press, 2009), 199-213. Billy Mitchell did not believe general air defense was possible but point defense was doable. Notably, Mitchell's system of point air defense depended upon a circle of surface and air surveillance posts extending in all directions for at least 150 miles from the protected locale. Mitchell recognized that Douhet was right, so Mitchell's system took steps to provide the speed of intelligence necessary to deprive an air attacker of an overwhelming initiative advantage. Mitchell's mode of defense was so resource intensive that it was unsuitable for national air defense.

speed ratio of intelligence to preparation for the defense was nearly unity. Consequently, air defenders could only react when the air attack's first blow was imminent or had already been felt, too late to parry the strike effectively. The invention of radar before WWII let defenders observe incoming air attacks at nearly the speed of light, making the speed ratio large once again such that effective general/area air defense became possible. However, the development of stealth technology in the 1970s and 1980s recalibrated the speed ratio of intelligence to preparation back to near unity, as it had been when Douhet first developed his air power theory.[4] Cyber power also inherently possesses a speed ratio of intelligence to preparation near unity because *all* action occurs near the speed of light in cyberspace. The use of air power during Operation Desert Storm displays the effect of a near unity speed ratio on the initiative in air warfare, similar to the dynamic observed in the Estonian and Georgian cyber attacks.

Another quality of air power that contributes to the advantage of initiative for attack is air power's mobility. This mobility creates a veil of uncertainty in three dimensions as to the vector of an air attack that radar largely lifted in WWII, but it is a veil that stealth has once again lowered in recent times.[5] Additionally, air power's mobility in the third dimension creates an advantage in concentric attack flowing from its ability to execute attacks in parallel from the enemy's center to his perimeter defenses.

As Sir John Slessor described in his air power theory, also penned during the Interwar Years, air power is an excellent tool with which to strike at an enemy's lines of communication.[6] Air power allows an attacker to strike at the enemy's rear area through a vertical flank attack, a flank that cannot be effectively defended if the speed ratio of intelligence to preparation is near unity as it was during Operation Desert Storm and at

[4] National Museum of the US Air Force, "Fact Sheet: Lockheed F-117A Nighthawk," 8 June 2007, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=410 (accessed 30 May 2011). By the 1970s it was possible to design stealth aircraft. The first F-117A flew on 18 June 1981.

[5] Stephen Bungay, *The Most Dangerous Enemy: An Illustrated History of the Battle of Britain* (Minneapolis, MN: MBI Pub. Co. and Zenith Press, 2010), 45-47. Under the management of Henry Tizard, Robert Watson-Watt and his team developed radar for Britain. After promising experimental results, the British Air Ministry deployed the Chain Home radar system to provide the rapid intelligence necessary to effectively defend their nation from enemy air attack.

[6] Slessor, *Air Power and Armies*, 122-23.

times during the WWII Combined Bomber Offensive, and as it is for cyber power.[7] In cyber power, the advantage of concentric attack is magnified as the cyber attacks in Estonia and Georgia show, because there are at least nine degrees of freedom in the cyber targeting problem.[8]

The concentric attack advantage of cyber power and air power depends first on an initiative advantage. Ever since radar's development, adversaries have waged electronic warfare to secure the air power initiative advantage. Like cyber warfare, electronic warfare also occurs near the speed of light, therefore it is virtually impossible to gain an initiative advantage by relying on increasing the speed of intelligence collection as radar did for air warfare. Consequently, the practitioners of electronic warfare have sought to drive the speed of preparation down. Rather than focusing on gathering intelligence *in* battle to gain the initiative advantage, electronic warfare practitioners rely on collecting intelligence *before* battle, decreasing the speed of preparation to almost zero in combat. If a number is divided by zero, the result is infinity. Therefore, no matter the speed of intelligence or if one is the attacker or defender, if one has countered an adversary's countermeasures *a priori*, the speed ratio of intelligence to preparation in warfare is by definition nearly infinite. As goes the contest for superior intelligence preparation, so goes the initiative advantage in air power.

As the Combined Bomber Offensive demonstrated during WWII, the initiative advantage in electronic warfare determined the initiative advantage in air warfare. In turn, intelligence generated, and electronic preparations made, before and between air battles determined the initiative advantage during the Combined Bomber Offensive. Hence, the initiative advantage in air power depended on an intelligence advantage before war to support superior preparations in electronic warfare. The Estonia and Georgia cyber attacks reveal that cyber power relies similarly upon intelligence to achieve an initiative advantage.

[7] Robert P. Givens, *Turning the Vertical Flank: Airpower as a Maneuver Force in the Theater Campaign*, CADRE Paper No. 13 (Maxwell AFB, AL: Air University Press, 2002), 81-85. The idea of thinking about air power, and by extension cyber power, as exhibiting the properties of flank attack stems from having read this work. The conclusion of the paper provides a good summary as to why conceptualizing air power as a flanking (maneuver) force is valid.

[8] See Chapter 2, page 21 to 23 for a detailed explanation of the nine degrees of freedom in cyberspace.

While intelligence before battle is critical for changing the speed of preparation to gain the initiative advantage in air and cyber power, there is an implicit assumption for land power regarding the initiative. This assumption is that the effects of attack are direct and thus a given, the destruction of the opposing force. If one does not know what the likely effects of a strike will be, the initiative is nearly worthless because there is too much uncertainty that one's actions will further one's war aim, the defeat of the enemy force.[9] In other words, if one is misoriented, one's ability to exploit the initiative to achieve victory is severely degraded.

For air and cyber power, the assumption that effects are direct is invalid. Cyber and air power naturally produce indirect and disruptive effects.[10] First, the targets for air and cyber power are often complex, networked systems that are reparable and changeable, although on different time scales. Cyberspace, the medium itself, is reparable and changeable.[11] By definition, attacks on any network that do not target every node in the system can only expect to create indirect effects.[12] As nodes are disabled or damaged, network performance degrades, disrupting the overall system. In complex networked systems that are reparable, attacks on the system generally only disrupt it because defenders can fix damage caused.[13] To paraphrase Slessor, air and cyber power "depend for [their] effect[s] far more upon dislocation and disorganization than upon actual material damage."[14] Network reparability has another implication in cyberspace – Slessor's dictum that the exercise of air power requires continuous effort also applies to cyber power.[15] Lastly, the indirect nature of air and cyber power impose a

---

[9] Clausewitz, *On War*, 75, 77. The aim of warfare is to disarm the enemy, to render him powerless. The aim is different from the political object, it is way that object is secured.

[10] Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 19-20. Slessor, *Air Power and Armies*, 122.

[11] Libicki, *Conquest in Cyberspace*, 5.

[12] Barabási, *Linked : The New Science of Networks*, 110-19. An often ignored property of complex systems is their vulnerability due to interconnectivity. The removal of nodes in a network leads to bottlenecks that degrade, and eventually disable a network. The removal of the node does not directly cause the network failure. A bottleneck is not a blockage. The blockage is a secondary effect to the direct outcome of node removal, which is reduced network capacity.

[13] Libicki, *Cyberdeterrence and Cyberwar*, 140-41. The effects of even the most fiendish cyber attacks can often be reversed within hours or, at most, weeks.

[14] Slessor, *Air Power and Armies*, 122.

[15] Slessor, *Air Power and Armies*, 136. "Immediately on receipt of the report of a successful attack on railway, arrangements should be made for the constant harassing, bombing by day and night, to prevent the junction being rendered fit for through traffic in as short a period as forty-eight hours."

need for information on system architecture and function in order to attack target networks with maximum indirect effect and efficiency, to avoid misorientation. Air and cyber power must therefore devote significant effort to intelligence preparation of the battlespace to orient satisfactorily and truly harness the initiative for victory. The Combined Bomber Offensive and air power in the Korean War reflect these dynamics in air power, which are also evident in the Estonian and Georgian cyber attacks.

Speed, Mobility, and Intelligence in Air Power

Operation Desert Storm demonstrates how air power's speed and mobility led to advantages in initiative and concentric attack. The Combined Bomber Offensive in WWII also demonstrates how air power's mobility created an advantage in concentric attack. This offensive also shows how one can use intelligence to decrease the speed of preparation to gain the initiative advantage in air warfare. Lastly, the Combined Bomber Offensive and air interdiction in the Korean War display how air power's initiative advantage depends on intelligence preparation of the battlespace because the effects of air attack are inherently indirect and of a disruptive nature.

Operation Desert Storm

Iraq's military invaded Kuwait on 2 August 1990 and, after a five-month build-up of coalition forces in Saudi Arabia, a coalition led by the United States launched Operation Desert Storm on 17 January 1991 to eject Iraqi forces from Kuwait.[16] The operation started with a month-long air campaign, before a 100-hour ground campaign led to Iraq's surrender and Kuwait's liberation.[17]

The operation's air campaign was based on a plan called Instant Thunder developed at the USAF Air Staff's Checkmate Division, which was led by Colonel John Warden.[18] The air campaign had three foci – Iraq's leadership, its military forces, and its infrastructure.[19] The campaign was divided into three phases with the following six

[16] U.S. Centennial of Flight Commission, "The Gulf War," http://www.centennialofflight.gov/essay/Air_Power/gulf_war/AP44.htm (accessed 30 May 2011).
[17] U.S. Centennial of Flight Commission, "The Gulf War."
[18] Richard G. Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, The USAF in the Persian Gulf War (Washington, DC: Air Force History and Museums Program, United States Air Force, 2002), 102.
[19] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 102.

objectives. First, destroy the Iraqi leadership's command and control.[20] Second, disrupt and attrit Iraq's elite military force, the Republican Guard.[21] Third, disrupt the Iraqi leadership's ability to communicate with its citizens.[22] Fourth, destroy key electrical grids and oil supplies.[23] Fifth, destroy Iraq's nuclear, chemical, and biological weapons capabilities.[24] Sixth, disrupt the Iraqi military's ability to resupply its forces in Kuwait.[25] By the end of the first phase, the plan anticipated that Iraq's leadership would have lost most of its ability to communicate with its populace or control its forces, as well as have significant difficulty reinforcing its army due to cuts in its lines of communication.[26]

F-117s and Tomahawk missiles carried out the initial wave of attacks on Iraq's capitol, Baghdad.[27] These attacks were launched before coalition air power disabled Iraq's integrated air defense.[28] The F-117s relied solely on electronic warfare, stealth technology and electronic attack in the form of radar jamming to seize the initiative and create surprise.[29]

The F-117s might have appeared as faint returns on Iraqi radars, so radar-jamming aircraft supported the air attack.[30] Jamming caused the Iraqi radar operators to turn down the gain on their displays to remove the jamming clutter such that any possible F-117 radar returns disappeared from the operators' scopes.[31] The combination of stealth and jamming drove the speed ratio of intelligence to preparation to almost unity for the Iraqis, and as Douhet described, effective defense against coalition F-117s was impossible. Without speed of light intelligence from radar, air power's speed was too great for Iraq's air defenses to react before the blow was delivered. No F-117s were lost

[20] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 104.
[21] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 104.
[22] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 104.
[23] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 104.
[24] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 104.
[25] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 104.
[26] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 105.
[27] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 182-97.
[28] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 183.
[29] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 183.
[30] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 186.
[31] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 186.

during the air campaign, or even effectively engaged by Iraqi fighters or surface-based air defenses.[32]

The Operation Desert Storm air campaign shows the initiative advantage created by air power's velocity when the defense's speed of intelligence is not much greater than its speed of preparation such that the defense cannot effectively react. In addition, the air campaign shows the concentric attack advantage created by air power's mobility. To begin with, one characteristic of concentric attack is that the defensive force is essentially fixed as a result of the encirclement, which allows the attacker to concentrate firepower on the target – a considerable advantage. Because of air power's speed and mobility, ground forces are essentially fixed relative to air forces. Consequently, defending ground forces on the front and their lines of communication are vulnerable to air attack simultaneously, just as if the defending ground force had been encircled or outflanked by an attacking ground force. This dynamic of concentric attack appears in the air barrage on Iraqi ground forces during Phases II and III of the Operation Desert Storm air campaign.[33]

Like a classic hammer-and-anvil flank attack, air power fixed Iraqi forces in Kuwait, cut them off from reinforcements and resupply, and destroyed them.[34] As the decimation of two Iraqi divisions at the Battle of Al-Khafji demonstrated, Iraqi mobile reserves could not move safely.[35] Like an effective land power flank attack, air power froze Iraq's reserve forces so that they could not use the advantage of interior lines to reinforce and concentrate against coalition land power.[36] As a result of the air interdiction campaign, Iraq's frontline forces suffered from shortages in food, water, medicine, and clothing, with many soldiers malnourished and in poor health.[37] Coalition air power cut off the lines of communication between Iraqi frontline forces and their supply depots in the rear, as if they were surrounded. Lastly, the destructive attacks on the fielded forces were devastating, as if by concentrated land firepower. When the 100-

[32] National Museum of the US Air Force, "Fact Sheet: Lockheed F-117A Nighthawk."
[33] Davis, *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, 104-05.
[34] Pape, *Bombing to Win: Air Power and Coercion in War*, 224.
[35] Pape, *Bombing to Win: Air Power and Coercion in War*, 244.
[36] Pape, *Bombing to Win: Air Power and Coercion in War*, 246.
[37] Pape, *Bombing to Win: Air Power and Coercion in War*, 248.

hour coalition land campaign against Iraqi forces in Kuwait started on 23 February 1991, air power had already decreased Iraqi troop strength to 41 percent with 20 percent of Iraqi armor and artillery destroyed.[38] Air power's natural speed ratio of intelligence to preparation near one, restored by stealth initially and later by the destruction or suppression of Iraqi radar, led to an initiative advantage for coalition air power that eventually permitted it to use its mobility and exploit the advantage of concentric attack against the Iraqi army in Kuwait. Together, these strategic advantages enabled air power to disaggregate and paralyze Iraqi forces in Kuwait such that they were easy prey for coalition land power.

Combined Bomber Offensive

The emergence of stealth air power during Operation Desert Storm can trace its roots back to the evolution of electronic warfare during the Combined Bomber Offensive of WWII. Before the development of radar, air attack had a dominant initiative advantage. The action-reaction cycle between belligerents trying to tilt the air power initiative in their favor stimulated the advent of electronic warfare during the Combined Bomber Offensive. These belligerents attempted to seize the initiative advantage by either maintaining the speed ratio of intelligence to preparation offered by radar when on defense, or, if on the attack, trying to decrease the ratio to unity as it had been before the use of radar.

Initially, the British assumed that their bombers would enjoy the initiative advantage that Douhet described under all conditions and embarked on a strategy of daylight bombing. However, they rapidly realized the initiative advantage held by German air defenses over their bombers conferred by radar after experiencing prohibitively heavy losses during daylight bombing raids.[39] For example, half the British bombers in two daylight raids in December 1939 were lost over the North Sea before they reached their targets.[40] At night however, the British learned that there were few

---

[38] Pape, *Bombing to Win: Air Power and Coercion in War*, 251.

[39] Randall T. Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command* (Toronto, Canada: University of Toronto Press, 2009), 21.

[40] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, Princeton Studies in International History and Politics (Princeton, NJ: Princeton University Press, 2002), 183-84.

German fighters to contend with and that anti-aircraft fire was ineffective.[41] The daytime losses compelled the British to rapidly adopt night bombing, which allowed them to temporarily regain the initiative.[42]

Soon the Germans introduced a significant night fighter force guided by ground controllers using radar intelligence to direct interceptors onto the attacking British bombers. By the end of March 1942, German night defenses were destroying, on average, four percent of attacking British bombers per raid, with German fighters accounting for two-thirds of the kills.[43] A four percent loss rate might seem insignificant, but compounded over time, a sustained four percent loss rate was enough to destroy all of British Bomber Command's fleet in just 112 sorties if the fleet could not be replenished. 112 sorties was not a lot for a total war like WWII. If Bomber Command's loss rate increased one percent, it would have been destroyed in just 90 sorties. An increase of one percent in loss rate would imply that the British aircraft industry would have to increase its production output by 20 percent to keep up with bomber attrition. Increasing aircraft production 20 percent would have been a non-trivial task with British industrial output already near its maximum. Although the introduction of German night fighters seemed relatively inconsequential, even a small diminishment of Bomber Command's initiative advantage and subsequent increases in bomber loss rates were significant for the British war effort.

To reduce its bomber loss rate, Bomber Command looked for vulnerabilities in the German night air defenses. Bomber Command realized that German defenses depended for success on the airborne *Lichtenstein* radar, the *Freya* early warning ground radar, the *Wurzburg* ground control radar, as well as communication between interceptor pilots and ground controllers.[44] All of these elements were vulnerable to electronic warfare jamming to some degree.[45] However, to exploit these vulnerabilities, British

[41] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 184.

[42] Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command*, 21.

[43] Alfred Price, *Instruments of Darkness: The History of Electronic Warfare* (New York, NY: Charles Scribner's Sons, 1977), 70.

[44] Price, *Instruments of Darkness: The History of Electronic Warfare*, 70.

[45] Price, *Instruments of Darkness: The History of Electronic Warfare*, 70.

intelligence needed to penetrate the veil of secrecy surrounding German radar technology.[46]

British intelligence hunted long and hard for the information it needed to exploit German radar vulnerabilities. For example, the British searched for more than one year before they finally possessed evidence of the *Freya* radar's existence in February 1941.[47] One year later, the British mounted Operation Biting to steal elements of a *Wurzburg* radar, from which Britain learned that the German radar had no built-in anti-jam capability, but that the system could be tuned over a wide range, which made electronic jamming difficult.[48] Additionally, the British victory at El Alamein in North Africa produced a windfall of technical intelligence on German radars, because Bomber Command obtained and reconstructed working *Freya* and *Wurzburg* radars for testing and exploitation.[49] Lastly, in August 1942 an electronic intelligence aircraft successfully collected data on the *Lichtenstein* airborne radar for Bomber Command during a British bombing raid.[50] Then in December 1942, Bomber Command realized that thin metal strips of the same size, codenamed Window but better known as chaff today, could jam both *Wurzburg* and *Lichtenstein* radars.[51] After nearly three years of gathering and analyzing intelligence, Bomber Command developed a clear enough picture of German radar defenses to prepare electronic countermeasures to seize the initiative advantage.

Window jamming impressively altered the initiative advantage in favor of the British upon its introduction during the Combined Bomber Offensive. Before Window was used, the average Bomber Command loss rate was 4.7 percent.[52] During the first six raids using Window in July 1943, the British bomber loss rate fell to 3.1 percent, and 83 percent of the bombers attacked their targets.[53] The decrease in loss rate corresponded to a 34 percent increase for Bomber Command in the possible number of sorties for a fixed number of aircraft. Bomber Command was so effective during this period that in the first

[46] Price, *Instruments of Darkness: The History of Electronic Warfare*, 70.
[47] Price, *Instruments of Darkness: The History of Electronic Warfare*, 77.
[48] Price, *Instruments of Darkness: The History of Electronic Warfare*, 81-86.
[49] Price, *Instruments of Darkness: The History of Electronic Warfare*, 93-95.
[50] Price, *Instruments of Darkness: The History of Electronic Warfare*, 107-08.
[51] Price, *Instruments of Darkness: The History of Electronic Warfare*, 164.
[52] Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command*, 139.
[53] Price, *Instruments of Darkness: The History of Electronic Warfare*, 163.

two raids on Hamburg that razed the city center, a mere 29 aircraft were lost in 1,513 sorties (1.9 percent).[54] Using intelligence to be better prepared *before* battle, Bomber Command had seized the electronic warfare initiative advantage and thus the initiative in air power as well.

In electronic warfare contests, better preparation largely determines the initiative because the speed of intelligence and the speed of action are the same, the speed of light. British radar countermeasures prepared in advance made German speed of light radar intelligence useless by overloading the radars with data that temporarily slowed the speed at which these systems produced intelligence to irrelevance. Effectively, through intelligence preparation before battle, the British returned the German air defense's speed ratio of intelligence to preparation to the Interwar, pre-radar value near unity. Hence, the British air attack enjoyed a tremendous initiative advantage over German defenses. By the beginning of August 1943, Bomber Command jamming had reduced the German night fighter force to near impotence.[55]

Bomber Command's dramatic initiative advantage was temporary. The Germans operationally and technically improved their air defenses from November 1943 to March 1944 to counter British radar and communications jamming, and almost defeated Bomber Command in the Battle of Berlin.[56] During the final British air attack in the Battle of Berlin, the Germans inflicted a loss rate of 11.8 percent on British bombers – a pace that Bomber Command could never sustain.[57] The British aircraft industry would have had to increase production by 62 percent to keep pace with such long-term operational losses. Yet, it took the Germans eight months of intelligence effort to perfect its new operational tactics and field new hardware to achieve these air defense results.[58] Like the British, the Germans could only seize the electronic warfare initiative advantage through prior intelligence that led to better *preparation*. These efforts briefly restored the German initiative advantage in electronic warfare by making radar an effective real-time

---

[54] Price, *Instruments of Darkness: The History of Electronic Warfare*, 151-60.
[55] Price, *Instruments of Darkness: The History of Electronic Warfare*, 165.
[56] Price, *Instruments of Darkness: The History of Electronic Warfare*, 198. Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command*, 157.
[57] Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command*, 157.
[58] Price, *Instruments of Darkness: The History of Electronic Warfare*, 167-98.

intelligence collector and making potent air defense possible once again. The air power initiative advantage once more rested with air defense, as it did during the Battle of Britain before the electronic warfare contest began in earnest.

While intelligence to enable better preparation and create an air power initiative advantage was a central feature of the Combined Bomber Offensive for the British, the Allied effort needed intelligence on the architecture and function of German industry to effectively use that initiative. Although the British and American air forces both viewed German industry as a network of interdependent entities, they held different theories about how best to attack this network.

The US Army Air Forces believed that a fragile and intricate industrial web held modern nation-states together, and that by carefully attacking the right element at the base of the web, one could cause the entire system to collapse.[59] This approach rested on intelligence, a scientific analysis to evaluate the cascading, and thus indirect, effects of destroying key nodes in the enemy's economic system.[60] The plan for Operation Pointblank captured the US approach to the Combined Bomber Offensive in 1943.[61] Pointblank identified six essential target systems, comprising 76 precision targets that would gravely impair the German war effort if destroyed.[62]

Although the British did not share the American view of the modern state's fragility, the preferred British bombing strategy viewed the enemy state as a networked system nonetheless. The British strategy was based on intelligence that indicated the general dislocation of industry by mass attacks on industrial centers would greatly impair German industrial capacity and enough destruction and dislocation would eventually lead to victory.[63] Both the British and US approaches sought to achieve victory by causing the

---

[59] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 160.

[60] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 160, 206.

[61] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 215-16.

[62] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 216.

[63] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 192, 199.

German war economy to implode through air attack on key nodes, but the two strategies differed on what they considered key nodes. US air forces considered key nodes to be precision targets. British air forces considered key nodes to be area targets, cities. Regardless of this difference, the British approach rested on at least coarse intelligence to identify and characterize industrial centers, and then evaluate the indirect and cascading (if any) effects of destroying these cities, or sections therein, on the German economy in order to prioritize targets.

However, the intelligence underpinning the British and American air strategies was flawed. Neither approach led the German war economy to collapse even though Allied air forces enjoyed an initiative advantage from superior electronic warfare and air superiority for much of the war. Still, German industrial production reached its highest levels of the war in 1944, just prior to its conclusion.[64] Clearly, this situation illustrates that an initiative advantage has less utility if one is disoriented so that the point of attack does not lead to the desired outcome. Yet, the Allied situation was less an intelligence failure than a reflection that air power's indirect effects propagate through a complex adaptive system, like a state's economy, in inherently unpredictable ways.

The air assault on German industry still created effects, albeit indirect and unintended ones. The Combined Bomber Offensive attacks on industry caused the Germans to disperse their factories in order to protect them from air attack.[65] Although the dispersion and dislocation of German industry did not lead to an economic collapse, they did compel the German economy to rely more upon transportation to integrate activities among these dispersed industrial nodes. The German transportation industry therefore became a more lucrative target air attack as an indirect, unintended consequence of the initial British and American air strategies.[66] Fortunately, senior Allied commanders directed their air forces to shift their focus onto transportation targets

[64] R. J. Overy, *The Air War, 1939-1945*, 1st ed., Cornerstones of Military History (Washington, DC: Potomac Books, Inc., 2005), 168. For example, German aircraft production in 1944 was nine percent greater than it was in 1941. Galbraith in Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 274. "Germany's total munitions output reached its peak in July 1944."

[65] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 286.

[66] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 286.

in March 1944 to prepare the battlefield for the D-Day invasion at Normandy.[67] Air attacks on the German transportation network eventually paralyzed the state's economy by the war's end.[68]

The Allied air attack on the German transportation system highlights how air power's mobility creates an advantage in concentric attack. The Allied air attack fixed German defense resources while simultaneously bombarding German lines of communication similar to a classic land power flank attack. The Combined Bomber Offensive fixed German anti-tank guns and the German air force in Germany where they could not affect the ground battles in France or Russia. Of the 19,173 dual-purpose anti-aircraft/anti-tank guns possessed by Nazi Germany, all but 3,172 were dedicated to air defense, depriving the German army of an essential tool for the ground fight.[69] The bulk of German fighter aircraft were concentrated in the rear to protect industry and cities in the Fatherland.[70] As a result, Allied air superiority was unchallenged during the Operation Overlord invasion of Normandy. Exploiting air power's mobility, Allied air forces attacked German cities and industry, and concurrently struck relentlessly at German rail and road transportation. When reinforcements flowed from the East to blunt the Allied assault in France, the disruption Allied air power created in the German transportation system caused it to take five days for an armored division to travel to a mere 200 miles, a distance easily traversable in one day if one averages a paltry fifteen miles per hour..[71] Consequently, German defenders in France were never reinforced to a

---

[67] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 234.

[68] Sebastian Cox as quoted in Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 286. Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 275, 280.

[69] *Crucible* cited in Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 285.

[70] Gunther Blumentritt, *von Runstedt: The Soldier and the Man* (London, UK: Odhams Press, 1952), 196, 223. The German Third Air Fleet was not in position to act decisively in the event the Allies invaded France, but Field Marshal von Runstedt was promised that air power reinforcements would be sent to France as soon as the invasion began. However, when the invasion occurred, von Runstedt's request for reinforcements to the Third Air Fleet was denied.

[71] Williamson Murray, *Luftwaffe* (Baltimore, MD: The Nautical and Aviation Publishing Company of America, 1985), 265.

degree sufficient to mount a successful counterattack.[72] The cascading effects of disruption in the German transportation network ensured that the German army in France was never able to reinforce beyond culmination.[73]

The Transportation Plan, the devastatingly effective attack on the German rail transportation network in 1944, was enabled by intelligence, which allowed Allied air power to exploit the initiative in harmony with the fact that the effects of air attack on networks are indirect. For instance, Solly Zuckerman, an advisor to the deputy commander of Allied forces in Europe, investigated the effects of air attack on the rail network in Sicily and southern Italy at the end of 1943.[74] Zuckerman's investigation helped identify and prioritize which rail nodes were the most lucrative targets given a rail network's architecture and function. Without this intelligence, brute force Allied air attacks on German railways might have paralyzed German transportation eventually, but in a very inefficient, lengthy, and costly manner. Effective and efficient exploitation of air power's initiative in the Combined Bomber Offensive depended upon intelligence preparation to understand how indirect effects would cascade through the rail network to the Allies' benefit.

Good intelligence facilitating satisfactory orientation, like that which underpinned the Transportation Plan, lets air power exploit the initiative to achieve desired results despite the fact that air power's effects are indirect. A similar lesson can be observed from the application of American air power against the Communists' transportation system during the Korean War.

Air Power in the Korean War

During the Korean War, air superiority, close air support, and air interdiction were the primary air power roles and missions. Air interdiction of North Korean lines of

[72] Max Hastings, *Overlord: D-Day and the Battle for Normandy*, 1st Vintage Books ed. (New York, NY: Vintage Books, 2006), 266. Allied fighter-bombers continually smashed German attempts to concentrate for a decisive armored counter-thrust.

[73] Clausewitz, *On War*, 566-73. Clausewitz defines culmination as the point beyond which effective self-defense is impossible. Air power ensured that during Operation Overlord, German forces in France were always at or beyond this point so that they could never effectively counterattack.

[74] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, 233. Solly Zuckerman was advisor to Air Chief Marshal Sir Arthur Tedder, General Eisenhower's deputy.

communication was both the greatest air power success and failure during the Korean War. Air power's triumph derived from an intelligence success in understanding the North Korean transportation system architecture and function at the start of the war. Air power's failure stemmed from an intelligence deficiency in understanding the North Korean transportation system architecture and function once China entered the war.

When the North Korean People's Army invaded South Korea in 1950, they drove the South Korean and US forces back on their heels. North Korean forces rapidly conquered South Korea save a small defensive enclave, the Pusan perimeter. General Douglas MacArthur's bold plan to bring in US Marine reinforcements to execute the Inchon flanking attack on the North Korean forces succeeded brilliantly. Just as rapidly, US forces beat back the North Korean army to the Yalu River on the Chinese border.

During MacArthur's rout of the North Korean army, air power performed brilliantly, particularly in its air interdiction role, attacking North Korean lines of communication, its rail and road network.[75] Like the Germans in WWII, North Korean forces were robbed of the supplies that allowed them to fight and could never mount a successful defense. The US air power success was based on satisfactory orientation, on intelligence about how rail and road transport system worked in modern societies. The North Korean transportation system at the start of the war was well understood, and thus air attack similar to that launched on the German transportation was just as successful.

However, all human activities share one characteristic – they are adaptive. When China entered the war, they adapted the transportation system to better support their forces engaged against the US military in Korea. One of the first innovations that the Chinese introduced was to leverage the concealment offered by night, and they performed most movements during this time[76] Second, readily available repair materials and abundant labor prevented US air power from knocking out any rail or roads

[75] Crane, *American Airpower Strategy in Korea, 1950-1953*, 40. "By night and day, aerial destruction rained down on on interdiction and strategic targets until almost all were destroyed by air attacks or overrun by advancing UN ground forces."

[76] Crane, *American Airpower Strategy in Korea, 1950-1953*, 41-42. "The interdiction campaign by Bomber Command and the Fifth Air Force was effective enough to force the enemy to make most movements at night…The inability to knock out moving ground targets at night would remain an Air Force deficiency through Vietnam."

completely.[77] For example, in December 1951 the Chinese had repair crews stationed at every rail junction and along every four miles of track.[78] These crews could repair damaged rail lines in as little as two hours and bridges in two to four days.[79] Lastly, when Chinese forces repatriated North Korea and the war settled into a stalemate in 1951, the pace of operations slowed and consumable usage rates dropped, so Chinese forces did not require large supply flows.[80] Altogether, these measures allowed the Chinese forces at the front to stockpile a supply cushion sufficient to sustain their forces for an extended period.[81] Consequently, when the US air interdiction campaign, Operation Strangle, cut rail traffic to five percent of capacity in 1951, the Communist transportation network still delivered 500 tons of supplies per day above what Chinese forces required.[82]

Despite the initiative advantage created by air power's speed and nearly complete air superiority, US air power did not deny Chinese forces sufficient supplies to bring them to defensive culmination because US air power was not oriented properly. Intelligence, colored by American predilections, led US military leaders to believe that the scarcity of North Korean and Chinese rail and truck transportation resources made these systems targets that could bring the Communist forces to their knees.[83] American intelligence failed to account for two factors that were the source of their misorientation. First, when the consumption rate of supplies is low and timeliness of delivery is unimportant, the inherent nature of air power effects (that they are disruptive vice destructive) means that attacks on lines of communication will be far less effective. Second, transportation networks are man-made and reparable. Rapid reparability can mitigate the effects of scarcity, particularly if the flow rate requirement through the transportation network is low. Misorientation, arising from faulty intelligence in understanding the architecture and function of the Communist transportation system, negated air power's initiative advantage in the latter half of the Korean War.

[77] Pape, *Bombing to Win: Air Power and Coercion in War*, 149-50. Crane, *American Airpower Strategy in Korea, 1950-1953*, 83.
[78] Pape, *Bombing to Win: Air Power and Coercion in War*, 150.
[79] Pape, *Bombing to Win: Air Power and Coercion in War*, 150.
[80] Pape, *Bombing to Win: Air Power and Coercion in War*, 149.
[81] Pape, *Bombing to Win: Air Power and Coercion in War*, 150.
[82] Pape, *Bombing to Win: Air Power and Coercion in War*, 151.
[83] Pape, *Bombing to Win: Air Power and Coercion in War*, 148, 150.

Speed, Mobility, and Intelligence – Cyber Power in Estonia and Georgia

Speed, mobility, and intelligence play similar roles in cyber power as they did for air power in WWII, the Korean War, and Operation Desert Storm. In the cyber attacks on Estonia and Georgia, the effects of speed and intelligence on initiative, of mobility on concentric attack, and of intelligence on orientation similar to those evident in air power's history appear.

As already described, in cyber power the speed ratio of intelligence to preparation is near unity, which tends to favor the attack, much like a near unity speed ratio favored the F-117 attacks in Operation Desert Storm. Like the Iraqi air defenders, the Estonian and Georgian cyber defenders did not know they were under attack until the virtual bombs began to land on their targets and the effects of the denial of service started to be felt.[84] The cyber defenders had no chance to *prevent* the effects of the cyber attack from being felt once it was launched, only to limit the effects *after* they manifested. For example, Estonian cyber defenders could not prevent banking and government websites from being defaced or the Internet from being disrupted, but Estonian cyber defenders did react to limit the effects, for example by raising a cyber drawbridge cutting off Internet access from the outside world.[85] However, through prior preparation facilitated by intelligence, the Estonian defense seized the initiative to beat back the cyber attackers.

The Estonian cyber defense had to react as the Germans air defense did in WWII when they were overwhelmed by British electronic jamming. The Germans fielded new technology resistant to British electronic jamming and developed new operational techniques to fight through Bomber Command's electronic attack. Four days after Estonia cut off access to its cyberspace from abroad and 11 days after the cyber attack started, Estonian cyber defenders had implemented a new operational concept to defend against the cyber assault. During this time, Estonia developed and deployed software to

---

[84] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 8. Lacking warning, Georgia only took mitigation actions after websites had been shut down. Davis, "Hackers Take Down the Most Wired Country in Europe." Shutdown of Estonian newspaper websites was the first indication that Estonia was under cyber attack. In both Estonia and Georgia, cyber defenders were not aware they were under attack until they had already experienced some attack effects.

[85] Davis, "Hackers Take Down the Most Wired Country in Europe." Ruus, "Cyber War I: Estonia Attacked from Russia."

filter out attacking Internet traffic, as well as deployed additional servers to increase their network capacity.[86] Moreover, the Estonians developed a new concept of operations. The cyber defenders set up online chat rooms so that all participants could readily share intelligence information real-time on attack targets and types.[87] The Estonian cyber defenders also traced the attacks back to their originating Internet protocol addresses and coordinated with Internet Service Providers to thwart the cyber attacks at their source.[88] Unlike air power, the malleability and the speed at which change can occur in cyberspace facilitate a much faster action-reaction cycle in the contest to seize the initiative through superior preparation. These cyber defensive countermeasures took days to weeks to deploy compared to the months German air defenses needed to adapt. Like it was for the German air defenders in the Battle of Berlin, preparation, not speed of intelligence, returned the initiative advantage to Estonia's cyber defense.

However, intelligence preparation of the battlespace gave the cyber attackers engaging Estonia the initiative advantage in the first place, as it did for Bomber Command in the development of Window during WWII. For example, the botnets employed in the cyber attack on Estonia used hijacked zombie computers, compromised by malicious Trojan-horse code unwittingly downloaded.[89] The attackers, having anticipated that Estonia might respond by cutting off Internet access from abroad, ensured that the ranks of hijacked computers included many within Estonia.[90] Additionally, the cyber attack leaders also recruited cyber militia members, script kiddies, residing in Estonia to continue the cyber attack even if the country were digitally walled off from outside Internet access.[91] The cyber attackers' preparations allowed them to continue the assault and retain the initiative advantage. Without these advanced preparations, the speed ratio of intelligence to preparation inherent to cyber power that

[86] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."
[87] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."
[88] Landler and Markoff, "In Estonia, what may be the first war in cyberspace."
[89] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24.
[90] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24. Evron and Aarleid, "Estonia: Information Warfare and Lessons Learned," 17-18. The cyber attackers targeting Estonia did not activate the zombies inside Estonia until after the country disabled Internet access originating from abroad.
[91] Guadagno, Cialdini, and Evron, "Storming the Servers: A Social Psychological Analysis of the First Internet War," 450. Vahe, "On the Front Lines of an Invisible War."

worked for the attackers would have worked against them. Once Estonia raised its cyber drawbridge, attack masters from abroad could not have hijacked botnet computers within Estonia as a reaction to Estonia's cyber defense. The attacking zombies within Estonia were only possible and effective because they were a *preparation* for, not a reaction to, the cyber defense. When Estonia took refuge within its fortress, the cyber attackers' preparations allowed them to retain the initiative and continue to press their cyber assault. The Estonian cyber conflict, attack-defense, action-reaction cycle demonstrates that the cyber power initiative advantage depends on preparation rooted in intelligence. The value of that initiative depends on how well one is oriented, which is also a function of intelligence.

The cyber attacks on Estonia and Georgia also display the effects of intelligence on orientation and the impact of orientation on attack effectiveness. Intelligence on Georgia's cyber architecture and function allowed the cyber attackers to maximize the indirect effects of their efforts. The cyber attackers assaulting Georgia appreciated the relationship between disruption, cascading effects, reparability, and required network capacity that US air planners missed in the Korean War. The cyber attackers concentrated their assault on just 54 targets, and the botnets used in the attack focused on just 11 targets.[92] In particular, the cyber attackers oriented properly on how Georgia might bring a cyber defense to bear and how the cyber attack's effects would cascade through Georgia's overall communication network. First, the attackers understood the effect of reparability on their distributed denial of service (DDoS) attack, which could also be considered cyber interdiction. The cyber attackers targeted, indirectly, the Georgian organization most able to repair and mitigate the effects of the cyber attack, Computer Emergency Response Team (CERT) Georgia. CERT Georgia was responsible the cyber security of Georgia's higher education institutions and was the nearest equivalent to a Georgian national computer emergency response team.[93] Attacking the Georgia's higher education institutions temporarily dislocated the country's best cyber defense force by directing its focus onto its charter responsibility, protection of militarily

---

[92] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 4. Botnets targeted 11 websites and script kiddies targeted another 43 for a total of 54 targets.

[93] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14-15.

irrelevant Georgian Research and Educational Network cyberspace. Channelizing CERT Georgia's attention away from the overall national cyber attack slowed the country's ability to repair its critical national cyberspace, even though the domain itself is rapidly reparable. Second, the cyber attackers appreciated that the effects of cyber power are primarily indirect and disruptive. The cyber attackers appreciated what impact disruption in cyberspace would have on the interrelated Georgian communications network, of which the Internet was just one part. Lastly, the cyber attackers appreciated how the rate of information flow related to the magnitude of disruption's effects on that network. Accordingly, the disruptive effect of the cyber attacks on Georgia appeared largely as dislocated communications, shunting those that would have traveled via the Internet into more traditional information conduits. This attack was timed to coincide with physical combat operations in South Ossetia. The physical combat operations created a dramatic spike in volume and rate of communication network usage overall. This spike combined with the dislocation of Internet communications to more traditional forms, like mobile and land phones, created an information bottleneck that effectively jammed Georgia's overall communications network during the early stages of the war when communications were most critical.[94] Simultaneously, the attackers had neutralized GRENA's ability to relieve these disruptive effects fast enough to prevent or sufficiently mitigate the intended adverse consequences for Georgia in the near-term. By orienting properly and understanding the architecture and function of Georgian cyberspace *as well as* its interrelationship to the broader communications network, the attackers' cyber interdiction efforts successfully supported Russia's combined arms campaign against Georgia. As air power theorist Sir John Slessor described, the important effects of air interdiction are the cumulative effects of a stoppage.[95] The 2008 cyber attack on Georgia demonstrates the same is true for interdiction in cyber power.

The cyber attackers who targeted Estonia were not as well oriented as those who struck Georgia. Specifically, the Estonian cyber attackers' intelligence did not appreciate

[94] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 16. "[C]ountries [like Georgia] whose information communication technology availability is low suffer most in terms of efficiency of information flow." Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 6. The high volume of cyber attack traffic jammed many general communications links including e-mail, land phones, and cell phones.

[95] Slessor, *Air Power and Armies*, 122-23.

the impact of traffic flow-rate requirements on the success of interdiction. In spite of being highly integrated with the Internet (more than 90 percent of Estonians bank online) the average Estonian experienced no impact on his daily life from the cyber attack.[96] If over 90 percent of banking is conducted online but most citizens experienced no impact from the DDoS attacks, then it is probable that like the Chinese forces at the front in the Korean War the rate of interaction/data consumption for any individual Estonian citizen with banks was relatively low, and the timeliness of data access was generally unimportant. Without appreciating the effect of information flow rate on cyber interdiction success and accounting for the actual Estionan cyber data flow rate, it was unlikely that the DDoS attacks could have had any coercive effect on the Estonian government. Under these conditions the government probably would not have been convinced to return the Russian WWII memorial statue to the Tallin city center, the cyber attackers' objective, without a protracted cyber attack to bring the effects home to the nation's population. Although the 2007 cyber attack on Estonia was newsworthy, misorientation from intelligence failures made it unlikely that the cyber attackers could have successfully used cyber interdiction to achieve their objective in the near-term. Consequently, the cyber attack on Estonia can be better characterized as a nuisance than a serious attempt at coercion.

Regardless of the relative success of the cyber attacks on Estonia and Georgia, these conflicts demonstrate the effect of cyber power's mobility on the capability to apply concentric attack, both on the enemy as a whole and within cyberspace. As the attacks on both countries show, cyber power, like air power in the Combined Bomber Offensive and Operation Desert Storm, allowed the attacker to target the heart of the enemy state without first defeating its fielded forces. Cyber attack targets ranged from government institutions, to banking, to communications.[97] As cyberspace continues to interlace with the fabric of modern life, the ability for cyber power to leverage the advantage of concentric attack will increase. For example, cyber power has already demonstrated its

---

[96] Ruus, "Cyber War I: Estonia Attacked from Russia."

[97] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 5-6. Davis, "Hackers Take Down the Most Wired Country in Europe."

ability to disable modern automobiles.[98] It is logical to extrapolate that similar cyber power capabilities will soon target military vehicles. Therefore like air power, cyber power offers another means to open a new combat front and outflank an opponent to strike in his rear areas and at his lines of communication. Additionally, as the attacking botnet zombies within Estonia illustrate, cyber power allows an attacker not just to attack an enemy's rear area, but to originate attacks from *within* the enemy's rear area.[99] Hence, cyber power has the potential to be employed like saboteurs, but with the mass of a large army as the Estonia-based botnet illustrated in 2007. Within cyberspace though, one can also attack on multiple flanks. For instance, the cyber attackers targeting Georgia fought on at least two cyber fronts, the physical and the semantic. DDoS attacks in both countries used data to overwhelm the physical capacity of computer hardware to process and transmit data over the Internet. In parallel, website defacements during both attacks manipulated the code that forms cyberspace's semantic layer to pass misinformation, which generated additional communications traffic attempting to correct such misinformation.[100] Thus, the website defacement attacks on the semantic layer contributed to cyber interdiction by indirectly increasing the stress on Georgia's communication system.

The cyber attacks on Estonia and Georgia demonstrate how cyber power's mobility can be used to exploit the advantage of concentric attack. Furthermore, the Estonia and Georgia cases show how speed and intelligence interact to affect the advantage of initiative through prior preparation and the initiative's value through proper orientation. As shown in the examples from the Combined Bomber Offensive, the Korean War, and Operation Desert Storm, cyber power shares these characteristics with air power.

---

[98] Koscher et al., "Experimental Security Analysis of a Modern Automobile," 4.

[99] Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 123-24. Cyber attackers on Estonia used hijacked computers inside the country to continue their assault when Estonia severed its external Internet connections.

[100] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified,* 44. Website defacements were a component of the attacks on both Estonia and Georgia.

SOME LESSONS ON CYBER POWER

While learning from experience is good, learning from others' experience is even better.

General James M. Mattis
in *Fiasco* by Tom Ricks

Some have argued that cyber power is so distinctive that lessons from the physical warfighting domains of land, sea, and air are not transferrable.[1] Still, others may argue that cyber power can be understood best by comparing it to a single domain. However, both hypotheses suffer from extreme rigidity where reality is much more fluid. Cyber power is neither purely unique in its dynamics in war, nor is it primarily like any other single warfighting domain. Cyber power shares features with land, sea, and air power. By using elemental concepts, the similarities between cyber power and power within each of the physical domains comes into focus.

Comparing the cyber events in Estonia and Georgia during 2007 and 2008, to land, sea, and air power examples spanning conflict from World War II to Operation Desert Storm illuminates how the concepts of attack and defense relate for cyber power in war. Advantage in war between cyber attack and cyber defense is still governed by the same set of fundamentals that regulate warfare in the physical domains, but they are refracted through the lens of cyberspace's distinctive characteristics. Advantage between attack and defense, independent of domain, rests on seven factors: orientation, initiative, terrain, fortresses, concentric attack, popular support, and moral factors.[2] In turn, speed, mobility, intelligence, concealment, and persistence, all of which are more or less prominent in each of the physical domains, influence these seven factors. With respect to land power, cyber power shares properties whose effects on warfare are similar to the effects of mountainous terrain and fortresses as observed in the Battle of Monte-Cassino

---

[1] Libicki, *Cyberdeterrence and Cyberwar*, xiii.

[2] Clausewitz, *On War*, 363. Clausewitz identifies all of these save orientation, which he calls *coup d'oeil* but does not include in his list. Boyd, "Organic Design for Command and Control," 15-16. Boyd describes orientation as a process of implicit cross-referencing that shapes one's perceptions of patterns in the world.

and the role and functioning of the Pusan perimeter in the Korean War. Regarding sea power, cyber power's qualities of concealment and persistence resemble the qualities displayed by submarine warfare as practiced in both the Atlantic and Pacific oceans during WWII. When it comes to air power, the effects of speed, mobility, and intelligence displayed in WWII, the Korean War, and the 1991 Persian Gulf War resemble those observed for cyber power. The foregoing analysis demonstrates how the similarities between cyber power and the physical domains were born out during the Estonian and Georgian cyber conflicts.

The similarities between cyber power and land, sea, and air power confirmed by this study lead to several lessons based on accepted military theory. First, when viewed in light of the *levee en masse* character of cyber power and the accompanying ability to generate mass in cyberspace, enclaves, fortresses created by firewalls in cyberspace, could better be employed for attack and defense by using them in a system of mutual support like Clausewitz described for land power. Enclaves so related can place a cyber attack on one enclave at risk from flank attack from one or more supporting cyber fortresses. The relationship between the Estonian Computer Emergency Response Team and the Root Internet Service Providers is a good example of mutual support at the global level. However, military cyber units must develop the necessary reinforcing and supporting capabilities and relationships in peacetime. In a joint campaign with military forces operating in all the warfighting domains, a four-day, ad hoc, coordination delay like the one in Estonia is simply unacceptable. Additionally, military cyber enclaves should be strong enough to force the enemy to invest them, but not so strong or weak that they become irrelevant because the enemy simply avoids them. This will consume enemy resources and attrit his attack potential, as well as create opportunities to identify and characterize an assault. Enclaves should be designed in such a way that they dilute an adversary's attack potential as he progresses further into defended cyberspace. Furthermore, cyber defense operational concepts that rely on enclaves should not expect their walls to hold indefinitely, because the lessons of the *levee en masse* and mountain warfare show that these walls will fail, and the enemy will find a way inside. Rather than struggle against this lesson, cyber defenders should embrace it and design enclaves with the requirement that they limit damage enough, and hold long enough to raise

reinforcements for a direct counterattack, concentric counterattack, or some other countermeasure. Although the current trend in cyber defense is away from enclaves and fortresses, these are effective cyber defensive tools if these virtual fortifications are used properly.[3] General MacArthur used Fortess Pusan in this manner, and Estonia used its cyber fortress similarly, both succeeded.

Another lesson arising from land power's similarities to cyber power relates to cyberspace's mountainous character. Cyber terrain is mountainous for *both* the attacker *and* the defender. While attackers will probably find a way into the protected area in the long run, as they did in the Battle of Monte-Cassino and the Estonian and Georgian cyber attacks, the cyber defender may complicate the attacker's intelligence problem by exploiting cyberspace's inherent malleability. Particularly in a joint military operation, cyber defense can greatly benefit from dramatically altering the physical and syntactic layers of friendly cyberspace just prior to the start of imminent hostilities, as well as periodically during the campaign. While an attacker will probably find a lightly defended route in the long run, in lightning wars of the type America prefers to fight, time is scarce. Changing the composition of friendly cyberspace has the potential to turn time scarcity into an advantage by forcing the adversary to reorient his cyber attack, potentially delaying the attack enough to be irrelevant. Changing the composition of friendly cyberspace would restore complexity and fog to the enemy's cyber battlespace picture that pre-war intelligence previously rendered clear. The intelligence burden created for an attacker by cyberspace's complex, mountainous character is a quality the defense can and should exploit with cyber terrain changes. Cyber power's similarities to land power indicate that an active cyber defense, using a system of cyber fortresses to weaken a cyber attack and buy time for reinforcements to arrive would be an effective strategy.

The implications of cyber power's concealment and persistence as illuminated by sea power in WWII are two-fold. As Julian Corbett described, forces should be dispersed such that a single blow cannot destroy an entire force, but be near enough to render

[3] Pitsenbarger, interview by author.

mutual support and concentrate at the point of attack.[4] Corbett's description of concentration and dispersion in sea power would be impossible for widely dispersed ships without the benefits of concealment and persistence due to natural, naval speed limitations. The long intelligence preparation times for cyber power, due to its complexity, create friction that slows the speed of action leading up to a cyber conflict such that concealment and persistence function in cyber power for ends similar to submarine sea power. Concealment combined with persistence permits an attacker to be effective in spite of an extensive preparation time requirement. This dynamic was observed in the submarine wolf pack strategies employed during WWII. The dynamic was also present in the Estonian and Georgian cyber attacks where observations indicate considerable time was required for the attackers to overcome the intelligence burden and be effective. As the cyber attacks on Estonia and Georgia demonstrate, Corbett's lessons on concentration and dispersion are a valuable source of insight regarding the force disposition of cyber power.

Additionally, concealment combined with persistence lets one exploit moral factors for advantage. Cyber power has the potential to facilitate bold action that would otherwise be too risky to undertake, enabling new strategic options. German submarine warfare off America's coast during WWII, while overwhelmingly outnumbered and far from the safety of home waters, reveals this interaction. The bold Stuxnet cyber attack on Iran's nuclear program is a similar example in cyber power. Cyber power's concealment combined with persistence presented decision-makers with a survivable, yet effective option to retard Iran's nuclear ambitions that would have otherwise been too risky to achieve by land, sea, or air power. Furthermore, the survivability afforded by cyber power's concealment can induce a sense of futility in the cyber defense, such that defenders simply stop trying to challenge a cyber attack. As coercion theorist Robert Pape describes, when one perceives the probability of benefiting from an action to be very low, people are generally unwilling to pay even the opportunity costs of an attempt, even if they possess the capability to do so.[5] Such a dynamic was at play when the Japanese stopped trying to convoy war materiel from outlying islands to their home

---

[4] Corbett, *Some Principles of Maritime Strategy*, 132.
[5] Pape, *Bombing to Win: Air Power and Coercion in War*, 17.

islands in WWII under threat from US submarines.[6] A similar dynamic may have been at work during the cyber attack on Georgia in 2008 given that some Georgian network administrators made no attempt to defend their cyberspace.[7] Cyber power's inherent concealment qualities have the potential to create a sense of futility in the mind of a defender. Although cyber power theorist Martin Libicki questions the utility of cyber power as a coercive tool, cyber power's similarities to submarine sea power suggest otherwise.[8] To suggest that cyber power has no coercive value is to essentially argue that cyber power is not a tool for war. Unless one's military objectives include enemy annihilation, war itself is an act of coercion. Furthermore, the reductionist proposition that cyber power possesses little utility as a coercive tool ignores that coercion and war happen within a specific context. Like all instruments of power, the extent to which cyber power is coercive hinges on all of the contextual elements for a given situation. Cyber power has possible strength as a coercive tool, at least at the operational level of war, especially in achieving cyber superiority when a defender retains dormant cyber power capabilities.

Several lessons also emerge from a coincidence in characteristics between cyber and air power. Air and cyber power's mobility create the opportunity to attack an opponent on multiple fronts, at all depths during a conflict as air power showed in Operation Desert Storm and cyber power demonstrated during the Estonian and Georgian cyber conflicts. The rudimentary ability to exploit the advantage of concentric attack displayed during the 2007 and 2008 cyber conflicts suggests that cyber power's advantage as a flanking force will only grow more potent as cyberspace becomes more ubiquitous in human activities. This suggests that cyber attack schemes to generate enemy paralysis or incoherence based on John Boyd's military theory – like air power's simultaneous flank attacks on command and control, lines of communication, and fielded

---

[6] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 816-19.

[7] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14. Some attacked Georgian websites made virtually no changes to try to defend themselves.

[8] Martin C. Libicki, "Wringing Deterrence from Cyberwar Capabilities," in *William B. Ruger Chair Workshop*, 19-21 May 2010, (New Port, RI: U.S. Naval War College, 2010), 259. "Being invisible, cyber capabilities cannot be easily used for deterrence, much less compellence (aka intimidation)." Contrary to Libicki's intimation, submarine sea power shows that invisibility has its advantages in coercion.

forces largely paralyzed and disaggregated Iraqi forces in Desert Storm – will become more applicable to cyber power in the future.[9]

Cyber power, like air power, is imbued with a natural speed ratio of intelligence to preparation near unity, which implies that the initiative advantage in cyber power also rests on intelligence and preparation prior to combat, regardless of whether on attack or defense. The Combined Bomber Offensive taught this lesson as Britain's Bomber Command attackers and the *Luftwaffe* defenders engaged in an electronic warfare cycle of action and reaction to gain the air power initiative. An abbreviated version of this action-reaction cycle was observed between attack and defense during the Estonian cyber conflict as attackers adjusted and defenders adapted with technology deployments and new operational procedures. Moreover, cyber power initiative's dependence on intelligence and prior preparation implies that secrecy is critical to ensure the effectiveness of cyber weapons. Like Bomber Command's chaff innovation in WWII and electronic warfare weapons today, cyber weapons rely on secrecy for their effectiveness. Bomber Command refrained from using chaff until they could gain the most benefit from it, accepting greater losses in the interim. The reliance on secrecy in electronic warfare for air power suggests that those who wield military cyber power may choose to accept some level of cyber damage in peacetime, so that they may husband the initiative advantage in the event of war. In cyber power, intelligence preparation and denying the enemy intelligence preparation are equally important to seizing the initiative. In other words, zero-day exploits are a key to seizing the initiative in cyber power, on attack or defense – they should be guarded ferociously.[10]

Although intelligence decides the initiative advantage in cyber warfare through preparation, intelligence also affects orientation, which allows one to effectively and efficiently exploit the initiative. The difference in attack effects between the Estonian and Georgian cyber conflicts highlights the importance of orientation in cyber power. The attacks on both countries were similar in that each applied a cyber interdiction

---

[9] Boyd, "Patterns," 133-34. Boyd's theory teaches that one should seek victory by producing enemy paralysis and disharmony through maneuver and strikes that penetrate, splinter, isolate or envelop, and overwhelm an opponent.

[10] A zero-day exploit is a surprise action that leverages a previously unknown cyber vulnerability or capability for advantage.

strategy via distributed denial of service. In Estonia, failing to appreciate their targets' data timeliness and data flow rate requirements, the cyber attackers had little impact on the daily life of Estonians. Without producing such effects, it is unlikely that cyber power could have coerced Estonia in a conflict of such short duration. However in Georgia, the cyber attackers accounted for data timeliness and flow rate, as well as cyberspace's reparability, and used cyber power to achieve their objective. The cyber attack successfully jammed Georgian cyber and traditional forms of communications. The importance of orientation in cyber power bears likeness with the centrality of orientation for air power in the Korean War. When air power planners rightly oriented based on good intelligence preparation, their efforts helped conquer most of North Korea. When air power planners misoriented based on poor intelligence, two years of air interdiction could not coerce the Communists to accept US peace terms. Orientation is a concept explicitly introduced in John Boyd's theory of war. He identifies orientation as the most important step in military operations. Orientation in cyber power carries the same or more weight as it does for military operations in the physical domains. Cyber power acquisition and strategy must make generating sufficiently right orientation a priority, if not the highest priority.

Because the effects of cyber power and air power are naturally indirect, some degree of misorientation when using these forms of military power should be anticipated. The need for proper orientation to effectively use cyber power does not mean that misorientation can always be avoided. For instance in WWII, Allied air power was successful even though its initial air attacks on German industry were misoriented. The Allies expected German industry to collapse under the weight of bombing. Instead, German industry survived, and even thrived, when it was dispersed to mitigate the effects of bombing. The dislocation of German industry, however, produced an unintended consequence – the German transportation network became more essential. Therefore, when General Eisenhower ordered Allied air forces to attack the transportation system, despite objections from his air force commanders Carl Spaatz and Arthur Harris, air power wreaked havoc on the German war effort. This exemplar of air power in WWII suggests two implications for cyber power not observed in the Estonian and Georgian cyber conflicts based on cyber and air powers' similarities. First, attack on an inherently

complex system like an enemy's cyberspace may create unintended opportunities or centers of gravity ripe for exploitation as indirect attack effects disrupt and dislocate the enemy. This was what the air attacks on industry caused regarding the German transportation network. Those who wield cyber power should be alive to opportunities flowing from unintended effects and be ready to adapt to leverage them for maximum advantage. Second, cyber attacks and market forces have combined to create a trend for cyberspace to become more porous.[11] The result is that cyber defenders at present tend to rely far less on cyber fortresses as a primary security mechanism.[12] Cyber dispersion via cloud computing is the emerging paradigm, but like German industry, dispersed computing makes the information communication network more critical. This dynamic puts cyber defenders on the horns of a dilemma – present more lucrative targets for cyber attack by concentrating in cyber fortresses that are inherently vulnerable in the long-term due to cyberspace's complexity, or disperse friendly cyberspace making the network itself a lucrative target. The dilemma between concentration and dispersion that cyber power creates was described by Sir John Slessor in his air power theory, *Air Power and Armies*, published in 1935.[13] The military in particular should dampen its ardor for cloud computing in light of Slessor's teachings. Slessor's air power theory also implies that lessons regarding air superiority are relevant for attaining cyber superiority. Slessor describes the problem of air superiority as "how to deprive the enemy the ability to interfere effectively by the use of his own air forces."[14] Slessor also counsels that efforts toward air superiority should be directed towards dislocating and disorganizing the opposing air force.[15] Both of these lessons were followed by the cyber attackers that assaulted Georgian in 2008. In the cyber attack, centers of cyber expertise were targeted

---

[11] Pitsenbarger, interview by author.

[12] Pitsenbarger, interview by author.

[13] Slessor, *Air Power and Armies*, 209. Slessor describes the dilemma of concentration and dispersion using tanks and air forces, but that is not critical. What is critical is that there is a simultaneous threat to lines of communication and concentrated resources, regardless of the type of force that provides the threat. In Slessor's description of the dilemma, the tank threat to lines of communication pulls opposite to the air threat. Tanks, by raiding an enemy's lines of communication compels him to concentrate his maintenance and supply and thus create excellent and vulnerable targets for the air force and vice versa.

[14] Slessor, *Air Power and Armies*. 31

[15] Slessor, *Air Power and Armies*. 31-32

in the initial cyber barrage.[16] By targeting educational institutions, the cyber attackers dislocated Georgian cyber defenders by getting them to focus their efforts on those targets for which they were directly responsible, but which had little to no relevance in defending against the Russian military operation. The attackers recognized that their objectives were jeopardized by cyberspace's characteristic reparability and took steps to neutralize the Georgian forces most capable of countering the assault. However, the cyber superiority the attackers obtained was extremely fleeting, as Georgia rehosted websites on American servers to mitigate the attack's effects.[17] In consonance with Slessor's air power theory, this experience intimates that due to cyberspace's reparability, cyber superiority, like air superiority, requires continuous effort.[18]

Some might argue that cyber power's similarities to air power could imply that the same command and control schema of centralized control and decentralized execution applies. In the centralized control, decentralized execution schema, the US Air Force (USAF) has centralized most planning, decision-making, and weaponeering at a very high echelon, the numbered air force where the air operations center resides. Cyber power's quality of persistence suggests that such highly centralized control may not be the best schema, as it is for air power which is far more ephemeral. The USAF has adopted its method of command and control because air power's fleeting nature frequently prohibits air crews from developing a comprehensive situational awareness of an area. Air power planning requires a perspective that incorporates information accumulated over time generally unavailable to lower echelons precisely because of the flexibility conferred by air power's speed and mobility. However, cyber power combines air power's qualities of speed and mobility with sea power's persistence. Cyber power's persistence lets lower echelon units observe their target environment over the extended

[16] Bumgarner and Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*, 5-6. A Georgian hacking forum and Georgian higher education institutions were targeted. Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*, 14-15. Computer Emergency Response Team Georgia had a primary responsibility to protect higher education institutions' cyberspace. The team's initial reflex was likely to support their primary customer at the expense of responding to the national cyber attack, which was beyond their charter scope of responsibility.

[17] Korns and Kastenberg, "Georgia's Cyber Left Hook," 66-67.

[18] Slessor, *Air Power and Armies*. 34 "Air forces can only be destroyed or neutralized by an active and persistent offensive in the air." Likewise cyber superiority will require continuous effort, but whether that translates into persistent attack depends on the specific circumstances of the conflict.

period necessary to develop situational awareness and orientation for more independent planning and execution. For example, US submarine wolf pack commanders were simply assigned an operations area in WWII and those units, rather than the headquarters sending them out, planned their operations in detail.[19] Similar mission command approaches to command and control are possible in cyber power. Any rush to embrace mission command approaches to cyber power should be tempered by cyber power's potential to create unpredictably broad cascading effects due to the domain's complexity. Cyber power's persistence implies that an effective approach to command and control would allow for mission command, distributed command and control, when widely cascading effects are unlikely. However, cyber power command and control should be highly centralized, similar to air power, when there is significant potential for unpredictable or negative cascading effects, or a broad perspective unavailable to lower echelons is necessary.

The final lesson from the totality of the preceding discussion and analysis is that cyber warriors and security professionals would greatly benefit from studying military theory developed from the experience of land, sea, air, and space power. To date, cyber power has been under the exclusive purview of the technically savvy. However, many cyber warriors, despite their technical prowess, are unfamiliar with the lessons of military theorists like Carl von Clausewitz, Sir Julian Corbett, John Boyd, and Sir John Slessor that underpin the analysis in much of this work.[20] If cyberspace is to be treated as a warfighting domain, then the time has come to translate cyber power's technical jargon into the lexicon of war. As the commander of US Cyber Command, General Keith Alexander has said, combat in cyberspace occurs daily.[21] Unaware of these military thinkers' teachings, cyber warriors apply their lessons on warfare, gotten through the bloody sacrifice of humanity, rightly and mistakenly every day. The implications of

---

[19] Blair, *Silent Victory: The U.S. Submarine War against Japan*, 541-48. For both the German and American wolf packs, patrols were sent out in an area with operations conducted at the discretion of the pack commander. American wolf pack commanders planned their own operations for their patrol areas. Keegan, *Battle at Sea: From Man-of-War to Submarine*¸ 235-36. In contrast, U-Boat headquarters designated patrol positions and directed to maneuvers against convoys when U-Boats spotted them.

[20] Pitsenbarger, interview by author.

[21] GEN Keith B. Alexander, "Cyber Update: Thoughts on Active Cyber Defense –and– Concepts for a Secure Zone" (keynote address, RSA Conference, San Francisco, 17 February 2011), http://media.omediaweb.com/rsa2011/keynotes/webcast.htm?id=3-1 (accessed 10 May 2011).

cyber power's parallels to land, sea, and air power described up to this point only scratch the surface of the many insights cyber warriors can glean from the experience of war. This thesis represents just a start to the development of cyber power theory on its own terms, but in harmony with the lessons on attack and defense learned from the experience of centuries of armed conflict. Only by understanding how concepts like orientation, initiative, and concentric fires operate in cyberspace can militaries hope to deliberately and effectively integrate cyber power into joint operations. Moreover, cyber warriors cannot afford to blindly accept the proposition that cyberspace is so different from all other warfighting domains that lessons learned there hold little transfer value. This thesis should have effectively dispelled this proposition. In war, the price of relearning lessons that could have been absorbed from books is the blood of one's countrymen.

BIBLIOGRAPHY

Air Force Doctrine Document (AFDD) 3-12. *Cyberspace Operations*. 15 July 2010.

Arnoldy, Ben. "Cyberspace: new frontier in conflicts." *The Christian Science Monitor*, 13 August 2008, http://www.csmonitor.com/USA/Military/2008/0813/p01s05-usmi.html (accessed 17 January 2011).

Barabási, Albert-László. *Linked: The New Science of Networks*. Cambridge, MA: Perseus Pub., 2002.

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, Princeton Studies in International History and Politics. Princeton, NJ: Princeton University Press, 2002.

Blair, Clay Jr. *Hitler's U-Boat War: The Hunters 1939-1942*. New York, NY: Random House, 1986.

Blair, Clay Jr. *Silent Victory: The U.S. Submarine War against Japan*. Philadelphia, PA: J. B. Lippincott Company, 1975.

Blumentritt, Gunther. *von Runstedt: The Soldier and the Man*. London, UK: Odhams Press, 1952.

Boyd, John R. "Conceptual Spiral." (1992) In *A Discourse on Winning and Losing*. Atlanta, GA: Defense and the National Interest, 1987.

Boyd, John R. "Organic Design for Command and Control." In *A Discourse on Winning and Losing*, February 2005 ed. edited by Chet Richards and Chuck Spinney. Atlanta, GA: Defense and the National Interest, 1987.

Boyd, John R. "Patterns of Conflict." In *A Discourse on Winning and Losing*, 27 February 2005 ed. edited by Chet Richards and Chuck Spinney. Atlanta, GA: Defense and the National Interest, 1987.

Brate, Adam. *Technomanifestos: Visions From the Information Revolutionaries*. New York, NY: Texere, 2002.

Broad, William J., John Markoff, and David E. Sanger. "Israel Tests on Worm Called Crucial in Iran Nuclear Delay." *New York Times*, 15 January 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (accessed 17 January 2011).

Bumgarner, John, and Scott Borg. *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*. U.S. Cyber Consequences Unit, 2009.

Bungay, Stephen. *The Most Dangerous Enemy: An Illustrated History of the Battle of Britain*. Minneapolis, MN: MBI Pub. Co. and Zenith Press, 2010.

Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America: Redefining America's Military Leadership*. Washington, DC, 2011.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About it*. 1st ed. New York, NY: Ecco, 2010.

Clausewitz, Carl von. *On War*. Edited and Translated by Michael Eliot Howard and Peter Paret. New York, NY: Oxford University Press, 2006.

Corbett, Julian S. *Some Principles of Maritime Strategy*, Classics of Sea Power. Annapolis, MD: Naval Institute Press, 1988.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. *On Cyber Warfare*, Chatham House Report. London, UK: The Royal Institute of International Affairs, 2010.

Crane, Conrad C. *American Airpower Strategy in Korea, 1950-1953*, Modern War Studies. Lawrence, KS: University Press of Kansas, 2000.

Cronin, Audrey Kurth. "Cyber-Mobilization: The New *Levee en Masse*." *Parameters* 36, no. 2 (Summer 2006): 77-87.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, 21 August 2007, http://wired.com/politics/security/magazine/15-09/ff_estonia (accessed 3 January 2011).

Davis, Richard G. *On Target: Organizing and Executing the Strategic Air Campaign Against Iraq*, The USAF in the Persian Gulf War. Washington, DC: Air Force History and Museums Program, United States Air Force, 2002.

Department of Defense. *The National Military Strategy for Cyberspace Operations*. Washington, DC, 2006.

Department of Defense. *Quadrennial Defense Review*. Washington, DC, 2010.

Department of State. "Background Note: Estonia." http://www.state.gov/r/pa/ei/bgn/5377.htm (accessed 24 March 2011).

Department of State. "Background Note: Georgia." http://www.state.gov/r/pa/ei/bgn/5253.htm (accessed 26 March 2011).

Douhet, Giulio. *The Command of the Air*. Edited by Joseph Patrick Harahan and Richard H. Kohn. Tuscaloosa, AL: University of Alabama Press, 1998.

"Estonia fines man for 'cyber war'." *BBC News*, 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm (accessed 3 April 2011).

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs* 9, no. 1 (2008): 121-26.

Evron, Gadi, and Hillar Aarleid. "Estonia: Information Warfare and Lessons Learned." In *Workshop on Learning from Large Scale Attacks on the Internet - Policy Implications*. Brussels, Belgium: European Commission, 2008.

Georgian Research and Educational Networking Association (GRENA). official Web site http://www.grena.ge/eng/cert.html (accessed 27 March 2011).

Givens, Robert P. *Turning the Vertical Flank: Airpower as a Maneuver Force in the Theater Campaign*, CADRE Paper No. 13. Maxwell AFB, AL: Air University Press, 2002.

Graham, Dominick, and Shelford Bidwell. *Tug of War: The battle for Italy, 1943-1945*. New York, NY: St Martin's Press, 1986.

Guadagno, Rosanna E., Robert B. Cialdini, and Gadi Evron. "Storming the Servers: A Social Psychological Analysis of the First Internet War." *Cyberpsychology, Behavior, and Social Networking* 13, no. 4 (2010): 447-53.

Harding, Luke. "Protests by Kremlin as police quell riots in Estonia." *Guardian: The Observer*, 29 April 2007, http://www.guardian.co.uk/world/2007/apr/29/russia.lukeharding (accessed 3 April 2011).

Hastings, Max. *Overlord: D-Day and the Battle for Normandy*. 1st Vintage Books ed. New York, NY: Vintage Books, 2006.

Heinl, Robert Debs, Jr. *Victory at High Tide: The Inchon-Seoul Campaign*. Great War Stories, 3rd ed. 1979. Reprint, Charleston, SC: The Nautical and Aviation Publishing Company of America, 2002.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011, http://www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (accessed 13 January 2011).

Joint Publication (JP) 3-13. *Information Operations*. 13 February 2006.

Keegan, John. *Battle at Sea: From Man-of-War to Submarine*. Pimlico ed. London, UK: Pimlico, 1988.

Keizer, Greg. "Russian hacker 'militia' mobilizes to attack Georgia" *Network World*, 13 August 2008, http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html (accessed 17 January 2011).

Knorr, Eric, and Galen Gruman. "What cloud computing really means: The next big trend sounds nebulous, but it's not so fuzzy when you view the value proposition from the perspective of IT professionals." *InfoWorld*, 7 April 2008, http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 (accessed 27 May 2011).

Korns, Stephen W., and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* 38, no. 4 (2008): 60-76.

Koscher, Karl, Alexei Czeski, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. "Experimental Security Analysis of a Modern Automobile." In *2010 IEEE Symposium on Security and Privacy*, 16-19 May 2010. Oakland, CA: Center for Automotive Embedded Systems Security, 2010. http://www.autosec.org/pubs/cars-oakland2010.pdf (accessed 31 May 2010).

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 24-42. Washington, DC: National Defense University Press: Potomac Books, 2009.

Landler, Mark, and John Markoff. "In Estonia, what may be the first war in cyberspace." *New York Times*, 28 May 2007, http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html?pagewanted=1&_r=1 (accessed 24 March 2011).

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*, Project Air Force. Santa Monica, CA: RAND, 2009.

Libicki, Martin C. "Wringing Deterrence from Cyberwar Capabilities." In *William B. Ruger Chair Workshop*, 19-21 May 2010, 259-72. New Port, RI: U.S. Naval War College, 2010.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York, NY: Frank Cass, 2004.

Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberspace Strategy." *Foreign Affairs* 89, no. 5 (2010): 97-108.

Mahan, A. T., and John B. Hattendorf. *Mahan on Naval Strategy: Selections from the Writitns of Rear Admiral Alfred Thayer Mahan*, Classics of Sea Power. Annapolis, MD: Naval Institute Press, 1991.

Menn, Joseph. "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government." *Los Angeles Times.com*, 13 August 2008, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html (accessed 27 March 2011).

Merriam-Webster. "logic bomb." *Merriam-Webster Dictionary* (2011), http://www.merriam-webster.com/dictionary/logic%20bomb (accessed 27 May 2011).

Microsoft. "What is a botnet?" *Safety & Security Center: Computer Security, Digital Privacy, and Online Safety*, http://www.microsoft.com/security/resources/botnet-whatis.aspx (accessed 27 May 2011).

Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military*. Tuscaloosa, AL: University of Alabama Press, 2009.

Murray, Williamson. *Luftwaffe*. Baltimore, MD: The Nautical and Aviation Publishing Company of America, 1985.

National Geographic. "Estonia Map." http://travel.nationalgeographic.com/travel/countries/estonia-map/ (accessed 23 March 2011).

National Museum of the US Air Force. "Fact Sheet: Lockheed F-117A Nighthawk." 8 June 2007, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=410 (accessed 30 May 2011).

National Security Agency. *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments*. 8 June 2001, http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed 2 March 2011).

Nimmo, Ben. "Violence rocks Estonia as riots spread beyond Tallin." *M&C News.com*, http://www.monstersandcritics.com/news/europe/news/article_1297586.php/Violence_rocks_Estonia_as_riots_spread_beyond_Tallinn (accessed 3 April 2011).

North Atlantic Treaty Organization (NATO). "NATO's relations with Georgia." http://www.nato.int/cps/en/natolive/topics_38988.htm (accessed 29 May 2011).

Oltsik, John. "Russian Cyber Attack on Georgia: Lessons Learned?" *Network World*, http://www.networkworld.com/community/node/44448 (accessed 27 March 2011).

Overy, R. J. *The Air War, 1939-1945*. 1st ed, Cornerstones of Military History. Washington, DC: Potomac Books, Inc., 2005.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009.

Pape, Robert A. *Bombing to Win: Air Power and Coercion in War*, Cornell studies in political economy. Ithaca, NY: Cornell University Press, 1996.

Parker, Geoffrey. *The Military Revolution: Military Innovation and the Rise of the West, 1500-1800*. Cambridge, UK: Cambridge University Press, 1996.

Parker, Matthew. *Monte Cassino: The Hardest-Fought Battle of World War II*. New York, NY: Doubleday, 2004.

Poulsen, Kevin. "Hacker Disables More Than 100 Cars Remotely." *Wired*, 17 March 2010, http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/ (accessed 27 May 2011).

Price, Alfred. *Instruments of Darkness: The History of Electronic Warfare*. New York, NY: Charles Scribner's Sons, 1977.

Public Broadcasting Station. "People and Discoveries: Heisenberg states the uncertainty principle, 1927." *A Science Odyssey*, http://www.pbs.org/wgbh/aso/databank/entries/dp27un.html (accessed 27 May 2011).

Ratcliff, R. A. *Delusions of Intelligence: Enigma, Ultra and the End of Secure Ciphers*. New York, NY: Cambridge University Press, 2006.

Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." *International Affairs Review*, 4 April 2009, http://www.iar-gwu.org/node/65 (accessed 3 April 2011).

Ruus, Kertu. "Cyber War I: Estonia Attacked from Russia." *European Affairs*, no. Winter/Spring (2008), http://www.europeaninstitute.org/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html (accessed 24 November 2010).

Slessor, John Cotesworth. *Air Power and Armies*. Tuscaloosa, AL: University of Alabama Press, 2009.

Sloan, Bill. *The Darkest Summer: Pusan and Inchon 1950: The Battles that Saved South Korea--and the Marines--from Extinction*. 1st Simon & Schuster hardcover ed. New York, NY: Simon & Schuster, 2009.

Sun Tzu, and Samuel B. Griffith. *The Illustrated Art of War*. New York, NY: Oxford University Press, 2005.

Tikk, Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallin, Estonia: Cooperative Cyber Defense Centre of Excellence, 2008.

U.S. Centennial of Flight Commission. "The Gulf War." http://www.centennialofflight.gov/essay/Air_Power/gulf_war/AP44.htm (accessed 30 May 2011).

Vahe, Urmas. "On the Front Lines of an Invisible War." *Baltic IT&T Review*, http://www.ebaltics.com/00704599?PHPSESSID=8b81c5fl58bb827ald825148e4d07c54 (accessed 31 May 2011).

Wakelam, Randall T. *The Science of Bombing: Operational Research in RAF Bomber Command*. Toronto, Canada: University of Toronto Press, 2009.

Windrow, Martin. *The Last Valley: Dien Bien Phu and the French Defeat in Vietnam*. 1st Da Capo Press ed. Cambridge, MA: Da Capo Press, 2004.

Yarger, Harry R. *Strategy and the National Security Professional: Strategic Thinking and Strategy Formulation in the 21st Century*. Westport, CT: Praeger Security International, 2008.